

## 明 細 書

### デジタルコンテンツ配信システム

#### 技術分野

本発明は、ネットワークを用いて、サーバ装置から映像、音楽などの  
5 デジタルコンテンツと、デジタルコンテンツの利用を許諾するライセン  
スを配信し、ユーザが端末装置でデジタルコンテンツを利用するシステ  
ムに関し、特に、前記サーバ装置と前記端末装置間の通信において、不正にライセンスの複製や改ざんが行われることを防ぎつつ、通信切断発生時においてもライセンスの消失や二重配信をも防ぐシステムおよび装  
10 置に関する。

#### 背景技術

近年、音楽、映像、ゲーム等のデジタルコンテンツ（以下、コンテン  
ツと記述）を、インターネット等の通信やデジタル放送等を通じて、サ  
15 ーバ装置から端末装置に配信し、端末装置においてコンテンツを利用す  
ることが可能な、コンテンツ配信システムと呼ばれるシステムが実用化  
段階に入っている。一般的なコンテンツ配信システムでは、コンテン  
ツの著作権を保護し、悪意あるユーザ等によるコンテンツの不正利用を防止するため、著作権保護技術が用いられる。著作権保護技術とは、具体的  
20 的には、暗号技術等を用いて、ユーザがコンテンツを再生したり、記録  
メディアにコピーしたりといったようなコンテンツの利用を、セキュア  
に制御する技術である。

例えば、特許文献１には、コンテンツ配信システムの一例として、暗  
号化されたコンテンツ、利用条件、および、コンテンツ復号鍵を端末装  
25 置が、サーバ装置より受信し、改ざん検出を行った後、利用条件の適合  
検証を行い、すべての検証を満足したときのみコンテンツの復号を行い

出力するシステムが記載されている。

このように、従来のコンテンツ配信システムでは、サーバ装置からライセンス（利用条件とコンテンツ復号鍵の総称。利用権利とも呼ぶ）を端末装置に配信するが、その配信経路は一般的にインターネットなどの公衆回線を用いるため、ライセンスの盗聴および改ざんを防ぐ必要がある。つまり、利用条件の不正改ざんやコンテンツ鍵の流出を防止しなければならない。さらに、サーバ装置はライセンス配信先の認証も行う必要がある。つまり、サーバ装置が意図しない端末装置にライセンスを配信することも防止する必要がある。盗聴・改ざん防止と通信相手の認証を行うプロトコルはSAC（Secure Authenticated Channel）プロトコルと呼ばれ、例えば、SSL（Secure Socket Layer）がよく知られている（非特許文献1）。

また、通信装置・通信回線の故障や電源断などによる通信切断がライセンス配信中に発生した場合、そのライセンスが消失してしまう可能性がある。このような場合、購入したコンテンツを再生することができないといった不利益がユーザに発生する。例えば、特許文献2および特許文献3には、通信切断による通信データの消失を、データ再送によって回避するプロトコルが記載されている。

（特許文献1）：特許第3276021号公報

20 （特許文献2）：特開2002-251524号公報

（特許文献3）：特開2003-16041号公報

（非特許文献1）：A.Frier, P.Karlton, and P.Kocher, "The SSL 3.0 Protocol", [online], Netscape Communications Corp., Nov. 18, 1996, [平成15年1月17日検索], インターネット<URL: http://wp.netscape.com/eng/ssl3/draft302.txt>

しかしながら、SACプロトコルや通信切断対策プロトコルは、その

適用範囲を広げるために汎用性を重視し、それぞれ独立に提案されている。これにより、双方のプロトコルを利用することで、ライセンスの盗聴・改ざんの防止、通信相手の認証、通信切断対策のすべての機能を実現するためには、双方のプロトコルで必要な通信往復回数が必要となる。

- 5       また、ライセンス取得やライセンス返却などのトランザクションを連続して行う場合、トランザクション毎にSACプロトコルと通信切断対策プロトコルを単純に繰り返すことにすれば、1回のトランザクション処理にかかる通信往復回数の倍数だけ通信往復回数が増えていくこととなる。例えば、1回のトランザクション処理にかかる通信往復回数を4
- 10   回とする場合、 $n$ 個のトランザクションを処理する際には $4n$ 回の通信往復回数が必要となる。

それゆえ、端末装置がトランザクション処理を完了するまでに通信遅延が発生し、ユーザが要求を出してから、応答を得るまでに待ち時間が発生するという課題がある。

15

#### 発明の開示

- 本発明の目的は、こうした従来の問題点を解決するものであり、ライセンスの盗聴・改ざんの防止、通信相手の認証、通信切断対策のすべての機能を実現するとともに、複数トランザクション処理を行う場合において、サーバ装置・端末装置間の通信往復回数を減少させ、さらに、上記
- 20   機能を実現するためにサーバ装置と端末装置で管理・保持する情報が少ないプロトコルを実現するシステムおよび装置を提供することである。これにより、ユーザが要求を出してから、応答を得るまでの待ち時間を短縮させることが可能なコンテンツ配信システムを提供することを目的
- 25   としている。

上記目的を達成する端末装置は、要求メッセージの送信、応答メッ

セージの受信、1つのトランザクション完了を確定させるためのコミットメッセージの送信を含むトランザクション処理に基づいてサーバ装置からコンテンツの利用に対するライセンスを取得し、前記ライセンスに基づいて前記コンテンツの利用を制御する端末装置であって、現在のトランザクション処理について処理中であるか処理済みであることを示す1ビットのトランザクション識別フラグを保持する保持手段と、連続する複数回のトランザクション処理における最終回を除く各トランザクション処理においてコミットメッセージを送信しないで、2回目以降の要求メッセージの送信時に、コミットメッセージの代わりに前記トランザクション識別ビットを送信する送信手段とを備える。

また、上記目的を達成するサーバ装置は、要求メッセージの受信、応答メッセージの送信、1つのトランザクション完了を確定させるためのコミットメッセージの受信を含むトランザクション処理に基づいて端末装置にコンテンツの利用に対するライセンスを提供するサーバ装置であって、連続する複数回のトランザクション処理における2回目以降の要求メッセージと共に前記コミットメッセージの代わりに送信される1ビットのフラグであって、端末装置においてトランザクションを処理中であるか処理済みであることを示すトランザクション識別フラグを受信する受信手段と、受信されたトランザクション識別フラグに基づいて1つのトランザクションの完了を確定するか否かを判定する判定手段とを備える。

この構成によれば、端末装置とサーバ装置とを含むコンテンツ配信システムで複数トランザクション処理を行う場合、要求メッセージと同時にコミットメッセージの代用としてトランザクション識別フラグを送信する。つまり、従来別々に送信される前後する2つトランザクション処理のコミットメッセージと要求メッセージとを、上記構成では1つのメ

ッメッセージに重ねて送信している。このように、コミットメッセージを送信しないのでサーバ装置と端末装置との間のメッセージ往復回数を減少させることができる。さらに、サーバ装置および端末装置で1ビットのトランザクション識別フラグという少ない情報量で、メッセージ往復回数  
5 数の削減と同時に通信切断対策を同時に行うことができる。これにより、ユーザがコンテンツ利用要求を出してから、応答を得るまでの待ち時間を短縮させることができる。

ここで、前記端末装置は、前記複数のトランザクション処理においてサーバ装置から送信される各応答メッセージを受信する応答受信手段と、  
10 応答受信手段による受信結果に従って、前記保持手段に保持されたトランザクション識別フラグを更新する更新手段とを備える構成としてもよい。また、前記更新手段は、前記サーバ装置に保持されるトランザクション識別フラグと同じ値を、保持手段に保持されるトランザクション識別フラグの初期値として設定し、応答受信手段によって応答メッセージ  
15 が受信されたとき、保持手段のトランザクション識別フラグの値を反転する構成としてもよい。

ここで、前記サーバ装置は、前記トランザクション識別フラグは、端末装置によってトランザクションが処理される毎に反転された値を有し、前記サーバ装置は、さらに、前記複数のトランザクション処理における  
20 前回の要求メッセージと共に送信されたトランザクション識別フラグのコピーである第1フラグを保持する保持手段を備え、前記判定手段は、受信手段によって受信された現在のトランザクション処理におけるトランザクション識別フラグと、保持手段に保持された第1フラグとが不一致であるとき、前回のトランザクションの完了を確定すると判定する構  
25 成としてもよい。

この構成によれば、サーバ装置内の判定手段は、前回のトランザクシ

ョン識別フラグのコピーである第1フラグと、受信された現在のトランザクション識別フラグとを比較することにより、端末装置において前回のトランザクション処理が完了したか否かを判定することができる。

ここで、前記端末装置は、前記トランザクション識別フラグの初期値は、前記複数のトランザクション処理においてサーバ装置から送信される初回の応答メッセージに含まれ、前記更新手段は、応答受信手段によって初回の応答メッセージが受信されたとき、保持手段のトランザクション識別フラグを初期値に設定し、応答受信手段によって応答メッセージが正常に受信されたとき、保持手段のトランザクション識別フラグの値を反転する構成としてもよい。

ここで、前記サーバ装置は、前記複数のトランザクション処理における初回の応答メッセージとともに、第1フラグの初期値を前記トランザクション識別フラグの初期値として、端末装置に送信する応答送信手段を備える構成としてもよい。

この構成によれば、サーバ装置内の判定手段は、第1フラグと、受信された現在のトランザクション識別フラグとが一致する場合は、端末装置におけるトランザクション処理の状態が変化していないので、トランザクション処理が完了していないと判定し、不一致である場合は、端末装置におけるトランザクション処理の状態が変化しているので、トランザクション処理が完了したと判定する。このように、サーバ装置は、コミットメッセージを受信しなくても、トランザクション識別フラグにより簡単に端末装置におけるトランザクション処理状態(完了したか否か)を簡単に判定することができる。

ここで、前記端末装置における要求送信手段は、前記応答受信手段によって応答メッセージが正常に受信されなかったとき、反転されていないトランザクション識別ビットを、現在のトランザクション処理の要

求メッセージとともに再度送信するように構成してもよい。

ここで、前記応答送信手段は、判定手段によって前回のトランザクションの完了を確定しないと判定されたとき、前回のトランザクション処理の応答メッセージを再度送信する構成としてもよい。

- 5      この構成によれば、例えば、通信切断という事故により端末装置が応答メッセージを正常に受信できなかった場合に、トランザクション処理を再開することができる。さらにサーバ装置は、誤った課金を防止するなどの通信切断対策を講じることができる。

- 10      ここで、前記端末装置は、複数のトランザクション処理における初回のトランザクション処理の直前にサーバ装置との間で相互認証する処理を行い、前記端末装置は、さらに、サーバ装置が端末装置を認証するための第1認証情報を認証要求として送信手段に提供し、応答受信手段によって前記第1認証情報に対する応答として受信された、端末装置がサーバ装置を認証するため第2認証情報を検証し、検証の結果、相互認証  
15      を確定させるための確定メッセージを送信手段に提供する認証手段を備え、前記送信手段は、前記確定メッセージを、前記初回のトランザクション処理の要求メッセージと共に送信する構成としてもよい。また、前記サーバ装置は、前記複数のトランザクション処理中の初回のトランザクション処理の直前にと端末装置との間で相互認証する処理を行い、前  
20      記サーバ装置は、さらに、受信手段によって認証要求として受信された、サーバ装置が端末装置を認証するための第1認証情報を検証し、正当と検証されたとき、端末装置がサーバ装置を認証するため第2認証情報を提供する認証手段を備え、前記要求受信手段は、前記初回の要求メッ  
25      ージと共に、相互認証を確定させるための確定メッセージを受信するように構成してもよい。

この構成によれば、サーバ装置および端末装置は、上記認証により確

立されたセキュアな通信路を介して複数のトランザクション処理を行うので、上記の通信切断対策に加えて、正規な端末装置に見せかけるなりすましや、メッセージの改ざんや、メッセージの盗聴を防止することができる。

- 5       ここで、端末装置は、前記複数のトランザクション処理を相互認証がなされたセッションと同一のセッション上で行う構成としてもよい。

この構成によれば、 $n$ 個のトランザクション処理を行う場合に、従来は $4n$ 回程度の通信往復回数を要していたところ、通信往復回数を $n+2$ 回にまで低減することができる。

- 10       以上のように本発明の端末装置およびサーバ装置によれば、ライセンスの盗聴・改ざんの防止、通信相手の認証、通信切断対策のすべての機能を実現するとともに、複数トランザクション処理を行う場合においても、サーバ装置・端末装置間の通信往復回数を減少させることができる。さらに、上記機能を実現するためにサーバ装置と端末装置で管理・保持する情報が少ないプロトコルを実現することができる。これにより、ユーザが要求を出してから、応答を得るまでの待ち時間を短縮させることができる。
- 15

#### 図面の簡単な説明

- 20       図1は、本発明の一実施形態に係るコンテンツ配信システムの構成を示すブロック図である。

図2は、本発明の一実施形態に係るコンテンツ配信装置のセキュリティ管理／通信部の詳細な構成を示すブロック図である。

- 25       図3は、本発明の一実施形態に係るユーザ端末のセキュリティ管理／通信部の詳細な構成を示すブロック図である。

図4は、本発明の一実施形態に係るコンテンツ配信システムで行われ



るコンテンツ購入に関する処理を説明するフローチャートである。

図 5 は、コンテンツ権利データベース 19 に格納されているコンテンツに関する情報の一例を概念的に示す図である。

図 6 は、ユーザデータベース 18 に格納されているユーザ情報の一例  
5 を概念的に示す図である。

図 7 は、ユーザ所有権利データベース 20 に格納されているユーザが所有する権利の情報の一例を概念的に示す図である。

図 8 は、コンテンツデータベース 21 に格納されているコンテンツ情報の一例を概念的に示す図である。

10 図 9 は、本発明の一実施形態に係るコンテンツ配信システムで行われるコンテンツ利用に関する処理を説明するフローチャートである。

図 10 A は、コンテンツ配信装置 1 とユーザ端末 3 との間で複数のトランザクション処理を行う 4 種類の通信フェーズを示す説明図である。

図 10 B は、コンテンツ配信装置 1 とユーザ端末 3 との間で複数のト  
15 ランザクション処理が正常に実行される場合のトランザクション識別ビットの遷移を示す説明図である。

図 10 C は、コンテンツ配信装置 1 とユーザ端末 3 との間で応答メッセージが届かなかった場合のトランザクション識別ビットの遷移を示す説明図である。

20 図 10 D は、コンテンツ配信装置 1 とユーザ端末 3 との間で要求メッセージが届かなかった場合のトランザクション識別ビットの遷移を示す説明図である。

図 11 は、本発明の一実施形態に係るコンテンツ配信システムで行われるコンテンツ利用処理において、ユーザ端末 3 とコンテンツ配信装置  
25 1 との初期フェーズにて行われる処理を説明するフローチャートである。

図 12 は、本発明の一実施形態に係るコンテンツ配信システムで行わ

れるコンテンツ利用処理において、ユーザ端末 3 とコンテンツ配信装置 1 との初期フェーズ後、初回コマンド通信フェーズを開始する前にユーザ端末 3 において行われる処理を説明するフローチャートである。

図 1 3 は、本発明の一実施形態に係るコンテンツ配信システムで行われるコンテンツ利用処理において、ユーザ端末 3 とコンテンツ配信装置 1 との初回コマンド通信フェーズにて行われる処理を説明するフローチャートである。

図 1 4 は、本発明の一実施形態に係るコンテンツ配信システムで行われるコンテンツ利用処理において、ユーザ端末 3 とコンテンツ配信装置 1 とのコマンド通信フェーズにて行われる処理を説明するフローチャートである。

図 1 5 は、本発明の一実施形態に係るコンテンツ配信システムで行われるコンテンツ利用処理において、ユーザ端末 3 とコンテンツ配信装置 1 とのコミットフェーズにて行われる処理を説明するフローチャートである。

## 発明を実施するための最良の形態

### (実施の形態 1)

図 1 は、本発明の一実施形態に係るコンテンツ配信システムの構成を示すブロック図である。図 1 において、本発明の一実施形態に係るコンテンツ配信システムは、サービス提供者側であるコンテンツ配信装置 1 と利用者側であるユーザ端末 3 とが、ネットワーク等の伝送路で接続される構成である。

コンテンツ配信装置 1 は、コンテンツ購入処理部 1 1 と、ユーザ登録部 1 2 と、ユーザ権利登録部 1 3 と、ユーザ権利作成部 1 4 と、コンテンツ暗号化部 1 5 と、コンテンツ管理部 1 6 と、セキュリティ管理／通

信部 17 と、ユーザデータベース 18 と、コンテンツ権利データベース 19 と、ユーザ所有権利データベース 20 と、コンテンツデータベース 21 とを備えている。また、ユーザ端末 3 は、ユーザ指示処理部 31 と、端末情報記憶部 32 と、コンテンツ蓄積部 33 と、利用権利管理部 34  
5 と、利用権利データベース 35 と、セキュリティ管理／通信部 36 と、出力部 37 とを備えている。

まず、上記コンテンツ配信システムを構成するコンテンツ配信装置 1 およびユーザ端末 3 の概要を、以下に説明する。

コンテンツ配信装置 1 において、コンテンツ購入処理部 11 は、コン  
10 テンツ購入処理実行時に、コンテンツ権利データベース 19 に格納され  
ている各コンテンツの内容、利用条件および料金等の情報を、ユーザ端  
末 3 へ送信してユーザに提示する。また、コンテンツ購入処理部 11 は、  
ユーザによってコンテンツが購入された場合には、ユーザ端末 3 からユ  
ーザ情報（ユーザ ID、端末 ID、ユーザ名、電話番号等）を取得する  
15 と共に、必要な課金処理を行う。コンテンツ権利データベース 19 には、  
コンテンツ（映画や TV 放送等の動画、書籍や印刷物等の静止画、ラジ  
オ放送や朗読等の音声および音楽、ゲーム等）毎に、コンテンツ利用に  
関する 1 つ又は複数の情報が格納されている。

ユーザ登録部 12 は、コンテンツ購入処理部 11 で取得されたユーザ  
20 情報を、ユーザデータベース 18 に記憶して登録する。ユーザデータベ  
ース 18 には、コンテンツ購入を行ったユーザの情報が、累積的に記憶  
されている。

ユーザ権利登録部 13 は、ユーザ登録部 12 を介してコンテンツ購入  
処理部 11 から与えられる、ユーザが購入したコンテンツに関する情報  
25 を、ユーザが所有する権利としてユーザ所有権利データベース 20 に記  
憶して登録する。ユーザ所有権利データベース 20 には、ユーザが購入

したコンテンツの利用権利が記憶されている。

ユーザ権利作成部 14 は、ユーザ端末 3 から受けるコンテンツ利用要求に応じて、ユーザ端末 3 へ送信する利用権利（利用条件、コンテンツの復号鍵）を生成する。

- 5      コンテンツ暗号化部 15 は、ユーザ端末 3 へ送信するコンテンツの暗号化を行い、コンテンツデータベース 21 へ暗号化コンテンツの登録を行う。

- 10      コンテンツ管理部 16 は、ユーザ端末 3 へ送信する暗号化コンテンツをコンテンツデータベース 21 から検索し、セキュリティ管理／通信部 17 へ渡す。

セキュリティ管理／通信部 17 は、ユーザ端末 3 の認証、コンテンツ配信装置 1 とユーザ端末 3 との間の秘匿通信（盗聴・改ざんの防止と通信相手の認証を行う通信）、および通信切断対策を行う。セキュリティ管理／通信部 17 の構成および通信プロトコルの詳細については後述する。

- 15      ユーザ端末 3 において、ユーザ指示処理部 31 は、ユーザが入力する指示（コンテンツ購入要求やコンテンツ利用要求等の指示）を処理する。

端末情報記憶部 32 には、上述したユーザ情報（ユーザ ID、端末 ID、ユーザ名、電話番号等）が記憶されている。

- 20      コンテンツ蓄積部 33 には、購入によって取得された暗号化コンテンツが蓄積される。

- 25      利用権利管理部 34 は、コンテンツ利用要求に応答してコンテンツ配信装置 1 から送信されてくる利用権利を受信し、その内容に従って、対応するコンテンツの処理（暗号解読や利用条件に基づく再生等）を実行する。この利用権利は、利用権利データベース 35 に格納されて管理される。

出力部 37 は、例えばディスプレイ等の表示装置であって、利用権利

管理部 3 4 が実行する処理に応じてコンテンツの出力を行う。

セキュリティ管理／通信部 3 6 は、コンテンツ配信装置 1 の認証、コンテンツ配信装置 1 とユーザ端末 3 との間の秘匿通信（盗聴・改ざんの防止と通信相手の認証を行う通信）、および通信切断対策を行う。セキュリティ管理／通信部 3 6 の構成および通信プロトコルの詳細については後述する。

次に、コンテンツ配信装置 1 におけるセキュリティ管理／通信部 1 7 の構成の詳細について図 2 を用いて説明する。固有鍵情報記憶部 2 0 1 は、公開鍵暗号方式におけるコンテンツ配信装置 1 固有の公開鍵  $K D s$  が含まれるサーバ公開鍵証明書と、コンテンツ配信装置 1 固有の秘密鍵  $K E s$  と、認証局公開鍵証明書とを記憶する。サーバ公開鍵証明書はコンテンツ配信装置 1 の公開鍵  $K D s$  に認証局の署名が施されたものである。公開鍵証明書のフォーマットには、一般的な X. 5 0 9 証明書フォーマットを用いるものとする。公開鍵暗号方式および X. 5 0 9 証明書フォーマットについては、ITU-T 文書 X. 5 0 9 "The Directory: Public-key and attribute certificate frameworks" が詳しい。

乱数発生部 2 0 2 は、乱数の生成を行う。生成された乱数は制御部 2 0 4 へ渡される。

暗号処理部 2 0 3 は、データの暗号化、復号、署名生成、署名検証、セッション鍵生成用パラメータの生成、セッション鍵の生成を行う。データの暗号化および復号アルゴリズムには AES (Advanced Encryption Standard) を、署名生成および署名検証アルゴリズムには EC-D SA (Elliptic Curve Digital Signature Algorithm) を用いる。AES については National Institute Stand

ard and Technology (NIST)、FIPS Publication 197、EC-DSSAについてはIEEE 1363 Standardが詳しい。

5 暗号処理部203は、データの暗号化／復号を行う場合には、AES  
鍵と平文／暗号化データをそれぞれ入力とし、入力されたAES鍵で暗  
号化／復号したデータをそれぞれ出力する。また、署名生成／検証を行  
う場合には、署名対象データ／署名検証データと秘密鍵／公開鍵をそれ  
ぞれ入力とし、署名データ／検証結果をそれぞれ出力する。さらに、セ  
ッション鍵生成用パラメータの生成を行う場合には、乱数を入力とし、  
10 Diffie-Hellmanパラメータを出力する。また、セッション  
鍵の生成を行う場合、乱数とDiffie-Hellmanパラメ  
ータを入力とし、セッション鍵を出力する。ここで、セッション鍵の生成  
にはECDH (Elliptic Curve Diffie-Hellman) を用いる。ECDHのアルゴリズムは、上記のIEEE  
15 1363 Standardが詳しい。

制御部204は、ユーザ端末3の認証処理、ユーザ端末3と送受信す  
るデータの暗号化／復号、改ざんのチェックを行う。さらに、制御部2  
04は、トランザクションに1ビットのトランザクション識別ビットを  
割り当て、そのトランザクション識別ビットと通信ステップ情報を通信  
20 ログデータベース206に保存することにより、通信切断対策処理を行  
う。ここで、トランザクションとは、「利用権利の取得」や「利用権利の  
返却」などの処理単位を表す。

通信部205は、ユーザ端末3のセキュリティ管理／通信部36と通  
信を行う。

25 次に、ユーザ端末3におけるセキュリティ管理／通信部36の構成の  
詳細について図3を用いて説明する。固有鍵情報記憶部301は、公開

鍵暗号方式におけるユーザ端末 3 固有の公開鍵  $K_{Dc}$  が含まれる端末公開鍵証明書と、ユーザ端末 3 固有の秘密鍵  $K_{Ec}$  と、認証局公開鍵証明書を記憶する。端末公開鍵証明書はユーザ端末 3 の公開鍵  $K_{Dc}$  に認証局の署名が施されたものである。公開鍵証明書のフォーマットには、コンテンツ配信装置 1 と同様に X. 509 証明書フォーマットを用いる。

乱数発生部 302 は、乱数の生成を行う。生成された乱数は制御部 304 へ渡される。

暗号処理部 303 は、データの暗号化、復号、署名生成、署名検証、セッション鍵生成用パラメータの生成、セッション鍵の生成を行う。暗号処理部 303 の入出力は、コンテンツ配信装置 1 の暗号処理部 203 と同じである。

制御部 304 は、コンテンツ配信装置 1 の認証処理、コンテンツ配信装置 1 と送受信するデータの暗号化／復号、改ざんのチェックを行う。さらに、制御部 304 は、コンテンツ配信装置 1 が生成したトランザクション識別ビットと通信ステップ情報を通信ログデータベース 306 に蓄積することにより、通信切断対策処理を行う。

通信部 305 は、ユーザ端末 3 側のセキュリティ管理／通信部 17 と通信を行う。

次に、本発明の一実施形態に係るコンテンツ配信システムで行われるコンテンツ配信方法を、図 4 ～ 図 12 を参照して具体的に説明する。

図 4 は、本発明の一実施形態に係るコンテンツ配信システムで行われるコンテンツ購入に関する処理を説明するフローチャートである。図 5 は、コンテンツ権利データベース 19 に格納されているコンテンツに関する情報の一例を概念的に示す図である。図 6 は、ユーザデータベース 18 に格納されているユーザ情報の一例を概念的に示す図である。図 7 は、ユーザ所有権利データベース 20 に格納されているユーザが所有す

る権利の情報の一例を概念的に示す図である。図 8 は、コンテンツデータベース 21 に格納されているコンテンツ情報の一例を概念的に示す図である。図 9 は、本発明の一実施形態に係るコンテンツ配信システムで行われるコンテンツ利用に関する処理を説明するフローチャートである。

5 図 10 A ~ 10 C、図 11、図 12 は、本発明の一実施形態に係るコンテンツ配信システムで行われる秘匿通信と通信切断対策処理を説明するフローチャートである。

#### (1) コンテンツ購入処理

図 4 を参照して、コンテンツ配信装置 1 で提供されるコンテンツをユーザが購入する際に、コンテンツ配信システムで行われる処理を説明する。

ユーザ端末 3 では、ユーザが、コンテンツ購入に関する指示をユーザ指示処理部 31 へ出力する。ユーザ指示処理部 31 は、セキュリティ管理／通信部 36 を介して、指示に応じたコンテンツ購入要求をコンテンツ配信装置 1 へ発行する (ステップ S41)。

コンテンツ配信装置 1 では、ユーザ端末 3 から発行されたコンテンツ購入要求が、セキュリティ管理／通信部 17 を介してコンテンツ購入処理部 11 で受信される。コンテンツ購入処理部 11 は、コンテンツ購入要求を受信すると、コンテンツ権利データベース 19 から格納されているすべてのコンテンツに関する情報を取得し、セキュリティ管理／通信部 17 を介してユーザ端末 3 へ送信する (ステップ S42)。

ここで、コンテンツ権利データベース 19 には、例えば図 5 に示すような情報が格納されている。図 5 において、コンテンツ名は、コンテンツの名称であり、コンテンツ ID は、コンテンツを識別するために付される固有の番号である。利用条件は、通常使用される予め定めたデータ形式によって、コンテンツを利用できる具体的な条件を示すものである。



各コンテンツに設定される利用条件および金額は、１つであってもよいし、複数であってもよい。この例では、映画Ａというコンテンツには、再生回数による利用条件が設定されており、４００円を支払えば、映画Ａを２回観賞することができることを表している。

5       なお、利用条件には、上述した利用回数や利用時間以外にも、利用期間、記録媒体へのコピーや書面への印刷の可否等の様々な条件を使用することが可能である。

10       再び図４を参照して、ユーザ端末３において、コンテンツ購入処理部１１から送信されたコンテンツに関する情報（図５）が確認され、ユーザがいずれかのコンテンツの購入を決定した場合（ステップＳ４３，Ｙｅｓ）、ユーザ指示処理部３１は、コンテンツ購入決定通知（購入したコンテンツおよび選択した利用条件の情報を含む）と共に、端末情報記憶部３２に格納されているユーザ情報を、セキュリティ管理／通信部３６を介してコンテンツ配信装置１へ送信する（ステップＳ４４）。

15       コンテンツ配信装置１では、ユーザ端末３から送信されるコンテンツ購入決定通知およびユーザ情報を、セキュリティ管理／通信部１７を介してコンテンツ購入処理部１１で受信する。そして、コンテンツ購入処理部１１は、必要な課金処理を実行すると共に、購入されたコンテンツの情報とユーザ情報とを、ユーザ登録部１２へ送出する（ステップＳ４  
20       ５）。なお、課金処理は本発明の主眼ではないので、説明を省略する。

ユーザ登録部１２は、コンテンツ購入処理部１１から送出される購入されたコンテンツの情報およびユーザ情報を、ユーザ権利登録部１３へ転送すると共に、ユーザ情報をユーザデータベース１８に記憶して登録する（ステップＳ４７）。このとき、コンテンツ購入処理部１１から送出  
25       されるユーザ情報と同一の内容が、既にユーザデータベース１８に登録されている場合には、上述したユーザ登録は行われず（ステップＳ４

6、Yes)。

ユーザデータベース18には、例えば図6に示すような情報が格納される。図6において、ユーザIDは、ユーザを識別するために付される固有の番号である。ユーザ名は、ユーザの名前である。端末IDは、端末を識別するために付される固有の番号であり、1人のユーザが複数の  
5 端末を所有している場合等に利用される。電話番号は、ユーザを特定するために利用される。図6の例では、「ユーザID「0001」である「一郎」というユーザが、ID番号「1234567」の端末を利用する」という内容が、ユーザ情報として登録されている。

10 ユーザ権利登録部13は、購入によってユーザが所有することになるコンテンツ利用の権利を、ユーザ登録部12から与えられる購入されたコンテンツの情報とユーザ情報とに基づいて、ユーザ所有権利データベース20に記憶して登録する(ステップS48)。

15 ユーザ所有権利データベース20には、例えば図7に示すような情報が格納されている。図7において、ユーザIDは、ユーザデータベース18に登録されている情報である。コンテンツIDおよび利用条件は、コンテンツ権利データベース19に登録されている情報である。

上記処理によって、コンテンツの購入およびその購入に伴うユーザの所有権利の登録が完了する。

## 20 (2) コンテンツ利用処理

次に、図9を参照して、上述した処理によってユーザ所有権利データベース20にユーザ所有権利が登録された後、ユーザが購入したコンテンツを利用する際にコンテンツ配信システムで行われる処理を説明する。

25 ユーザ端末3では、ユーザが、コンテンツ利用に関する指示をユーザ指示処理部31へ出力する。このとき、ユーザは、コンテンツをどのように利用するのかの指示を与える。例えば、購入したコンテンツの利用

条件が回数であれば何回利用したいのか、時間であれば何分利用したいのかという指示を与える。ユーザ指示処理部 31 は、セキュリティ管理／通信部 36 を介して、指示に応じたコンテンツ利用要求をコンテンツ配信装置 1 へ送信する(ステップ S 9 1)。なお、コンテンツ利用要求は、

- 5 必ずしもユーザ指示に従って作成されるものではなく、ユーザ端末 3 内で自動的に作成される場合もある。例えば、端末 3 がサポートするコンテンツの利用条件が固定されている場合、ユーザが指示を与えるまでもなく、コンテンツ利用要求をユーザ端末 3 内で作成することができる。具体的には、ユーザ端末 3 が、記憶容量の制限により毎回 1 回分の利用
- 10 権利だけが取得・処理可能な端末の場合であり、この場合には端末に応じたコンテンツ利用要求をユーザ指示処理部 31 で自動的に作成し、コンテンツ配信装置 1 へ発行する。このコンテンツ利用要求には、上記指示の内容、ユーザ ID、端末 ID およびコンテンツ ID が含まれる。

- コンテンツ配信装置 1 では、ユーザ端末 3 から送信されたコンテンツ
- 15 利用要求を、セキュリティ管理／通信部 17 を介してユーザ権利作成部 14 で受信する。ユーザ権利作成部 14 は、コンテンツ利用要求を受信すると、この要求に対応した内容が登録されているか否かを、ユーザデータベース 18 およびユーザ所有権利データベース 20 を参照して確認する(ステップ S 9 2)。具体的には、ユーザ権利作成部 14 は、コンテ
- 20 ンツ利用要求に含まれるユーザ ID および端末 ID が、ユーザデータベース 18 に登録されているか否かをまず確認し、登録されていると判断すると、そのユーザ ID においてコンテンツ利用要求に含まれるコンテンツ ID および指示に応じた利用条件が、ユーザ所有権利データベース 20 に登録されているか否かを確認する。

- 25 上記ステップ S 9 2 における確認の結果、コンテンツ利用要求に対応した内容が登録されていると判断した場合(ステップ S 9 3, Yes)、

ユーザ権利作成部 14 は、コンテンツ利用要求に応じた利用権利を作成し、セキュリティ管理／通信部 17 を介してユーザ端末 3 へ送信する(ステップ S 9 4)。また、ユーザ権利作成部 14 は、コンテンツ利用要求に含まれるコンテンツ ID をコンテンツ管理部 16 へ通知する。コンテンツ管理部 16 は、コンテンツ ID に対応するコンテンツをコンテンツデータベース 21 から取り出し、セキュリティ管理／通信部 17 を介してユーザ端末 3 へ送信する(ステップ S 9 5)。

一方、上記ステップ S 9 2 における確認の結果、コンテンツ利用要求に対応した内容が登録されていないと判断した場合(ステップ S 9 3, N o)、ユーザ権利作成部 14 は、コンテンツ利用要求を拒絶する旨を、セキュリティ管理／通信部 17 を介してユーザ端末 3 へ通知する(ステップ S 9 7)。

ここで、上記ステップ S 9 4 で行われる利用権利の生成は、次のようにして行われる。前提として、ユーザ ID「0001」のユーザが、図 7 のユーザ所有権利データベース 20 に示される登録内容で、事前にコンテンツの購入を行っていたと仮定する。

さらに、そのユーザが、コンテンツ ID「112233」のコンテンツを 1 回利用したいというコンテンツ利用要求を送信してきた場合を考える。この場合、ユーザ所有権利データベース 20 に登録されている利用条件が 2 回であるので、ユーザ権利作成部 14 は、要求通り再生回数 = 1 を与える情報および該当コンテンツの復号鍵を含む利用権利を作成する。また、ユーザ権利作成部 14 は、この利用権利の作成と同時に、ユーザ所有権利データベース 20 に登録されている利用条件の回数を 1 つ減少させて、登録内容を更新する(図 7 の例では、2 → 1)。ただし、通信切断対策処理において、セキュリティ管理／通信部 17 から再開トランザクションとして指示された場合には、登録内容の更新を行わない。

なお、通信切断対策処理については後述する。

5      なお、ユーザ権利作成部 14 は、通信切断対策処理により再開トランザクションが発行されることを想定して、作成したユーザ権利を保存しておいてもよい。これにより、再開トランザクション発行時にユーザ権利を再度作成する手間を省くことができる。

10      なお、ユーザ端末 3 へ利用権利を発行する毎に、ユーザ所有権利データベース 20 に登録されている内容を更新した結果、コンテンツの購入によって与えられた利用条件がなくなった場合には、ユーザ所有権利データベース 20 に登録されている該当ユーザ所有権利を削除してもよいし、そのまま残しておいてもよい。残しておく場合には、同一のユーザが再度同じコンテンツの購入を行ったときや、ユーザが取得した利用権利を行使せずに返却するとき等に、処理対応がしやすくなる。

15      再び図 9 を参照して、ユーザ端末 3 において、コンテンツ配信装置 1 から送信される暗号化コンテンツは、コンテンツ蓄積部 33 に蓄積され、利用権利は、利用権利管理部 34 に入力される。利用権利管理部 34 は、取得した利用権利に含まれる復号鍵を用いて該当コンテンツに施された暗号を解読し、利用条件に従って暗号解読したコンテンツの再生処理等を、出力部 37 を通して実行する（ステップ S96）。なお、取得された利用権利は、利用権利データベース 35 に格納され、コンテンツの再生  
20      回数や累積時間等の管理に利用される。

上記処理によって、要求される利用条件に応じたコンテンツを配信することができる。

### （３）秘匿通信・通信切断処理

25      まず、図 10 A を参照して、上述したコンテンツ利用処理において、コンテンツの利用要求（図 9 のステップ S91）、および、利用権利とコンテンツの送信（図 9 のステップ S94、S95）が複数回行われる際

に、セキュリティ管理／通信部 17、36で行われる、認証処理、利用  
権利の盗聴・改ざん防止処理、および通信切断対策処理の概略を説明す  
る。

ユーザ端末 3 とコンテンツ配信装置 1 との通信は、すべてユーザ端末  
5 3 から開始されるリクエストメッセージと、前記リクエストメッセージ  
に呼応してコンテンツ配信装置 1 から返信されるレスポンスメッセージ  
からなる。リクエストとレスポンスとの対をフェーズと呼び、秘匿通信・  
通信切断処理は図 10 に示すとおり 4 種類のフェーズからなる。

初期フェーズ P 1 は、ユーザ端末 3 とコンテンツ配信装置 1 との間で  
10 セッションが確立された後、最初に 1 度だけ行われる相互認証用のフェ  
ーズである。この初期フェーズ P 1 について、初期フェーズ P 1 以前の  
トランザクションが正常に終了していた場合と、通信切断等により異常  
終了していた場合とに分けて初期フェーズ P 1 について説明する。

以前のトランザクションが正常に終了している場合、初期フェーズ P  
15 1 においてユーザ端末 3 は、コンテンツ配信装置 1 がユーザ端末 3 を認  
証するための認証情報 A を初回の要求メッセージとしてコンテンツ配信  
装置 1 に送信する。コンテンツ配信装置 1 は、認証情報 A を検証した後、  
ユーザ端末 3 がコンテンツ配信装置 1 を認証するため認証情報 B を送信  
する。その際、認証情報 B と共に、コンテンツ配信装置 1 からユーザ端  
20 末 3 に、トランザクション識別ビット T の初期値（例えば 0）が送信さ  
れる。ユーザ端末 3 が認証情報 B を検証した後、相互認証を確定させる  
ための認証情報 C は、単独で送信されないで、次の初回コマンド通信フ  
ェーズ P 2 における要求メッセージと共に送信される。また、以前のト  
ランザクションが通信切断等により異常終了している場合には、正常終  
25 了していた場合の上記の処理と比べて、コンテンツ配信装置 1 から送信  
されるトランザクション識別ビット T の値とトランザクションを再開す

る点とが異なる。すなわち、コンテンツ配信装置 1 は、正常に終了して  
いないトランザクションで用いていたトランザクション識別ビットの値  
をそのまま（つまり反転しないで）送信する。さらにコンテンツ配信装置  
1 は、次の要求メッセージを、異常終了した以前のトランザクションの  
5 再開トランザクションに対する要求とみなす。

初回コマンド通信フェーズ P 2 は、初期フェーズ P 1 に続いて 1 度だ  
け行われるフェーズである。初回コマンド通信フェーズ P 2 によって、  
最初のトランザクションが処理される。この初回コマンド通信フェーズ  
P 2 において、ユーザ端末 3 は、要求メッセージと共に、認証情報 C お  
よびトランザクション識別ビット T を送信する。ここで送信されるトラ  
ンザクション識別ビット T の値は、前回のトランザクション処理が正常  
に完了した場合コンテンツ配信装置 1 から送信されたトランザクション  
識別ビットを反転した値であり、完了していない場合には前回の（中断  
している）トランザクションで用いた値である。コンテンツ配信装置 1  
15 は、トランザクション識別ビットが反転している場合には、新たなトラ  
ンザクションの開始と判断して、要求メッセージに対する応答メッセー  
ジをユーザ端末 3 に送信する。また、コンテンツ配信装置 1 は、トラ  
ンザクション識別ビットが反転していない場合には、再開トランザクシ  
ョンと判断して、前回と同じ応答メッセージをユーザ端末 3 に送信する。  
20 正常に応答メッセージを受信したユーザ端末 3 は、連続してトランザク  
ション処理を行わない場合には、コミットメッセージを送信すること  
によりコミットフェーズ P 4 に移行する。また、正常に応答メッセージ  
を受信したユーザ端末 3 は、連続してトランザクション処理を行う場合  
には、コミットメッセージを送信しないで、次のコマンド通信フェーズ P  
25 3 a における要求メッセージと共にトランザクション識別ビット T を送  
信する。

コマンド通信フェーズ（P 3 a 等）は、同一セッション内で2つ以上のトランザクションを処理する場合に発生するフェーズである。つまり、コンテンツの利用要求および利用権利とコンテンツの送信が複数回行われる場合に、コマンド通信フェーズP 3 aが用いられる。コンテンツの利用要求および利用権利とコンテンツの送信が1度だけの場合は、コマンド通信フェーズP 3は行われず、コマンド通信フェーズP 3は、最初のトランザクションに続くトランザクション数だけ繰り返される。このコマンド通信フェーズP 3 aでは、コミットメッセージは送信されず、コミットメッセージの代わりにトランザクション識別ビットTが、次のコマンド通信フェーズ（P 3 b）における要求メッセージと共に送信される。

コミットフェーズは、すべてのトランザクション処理が終了した後にコンテンツ配信装置1においてトランザクション処理の完了を確定させるためのフェーズである。

図10Bは、図10Aに示した4つの通信フェーズにおいて、コンテンツ配信装置1とユーザ端末3との間で複数のトランザクション処理が通信切断なしに正常に実行される場合のトランザクション識別ビットTの遷移を示す説明図である。

トランザクション識別ビットTの初期値（例えば $T = 0$ ）は、初期フェーズP 1のレスポンスと共にコンテンツ配信装置1からユーザ端末3に送信される。コンテンツ配信装置1およびユーザ端末3はそれぞれ初期値を保持する。このトランザクション識別ビットTはユーザ端末3においてトランザクション処理が完了したときに反転される。

ユーザ端末3は、初期フェーズP 1のレスポンスとして、トランザクション識別ビットTと認証情報Cを受信したとき、トランザクション識別ビットTを反転する（ $T = 1$ ）。反転しているのは、特に異常している



トランザクションが存在しないからである。

次の初回コマンド通信フェーズP2においてユーザ端末3は、レスポンスを正常に受信したとき、トランザクション処理が完了したのものとしてトランザクション識別ビットTを反転する( $T=0$ )。次のコマンド通信フェーズP3aにおいてユーザ端末3は、レスポンスを正常に受信したとき、トランザクション処理が完了したのものとしてトランザクション識別ビットTを反転する( $T=1$ )。このようにして、ユーザ端末3は、レスポンスを正常に受信した場合に、トランザクション識別ビットTを反転する。

10 反転後のトランザクション識別ビットTは、次のコマンド通信フェーズの要求メッセージと共に送信されるので、コンテンツ配信装置1に、ユーザ端末3におけるトランザクション処理が完了したことを通知することになる。

15 初回コマンド通信フェーズP2において、コンテンツ配信装置1は、要求メッセージと共に受信したトランザクション識別ビットT( $=1$ )と保持している初期値T( $=0$ )とを比較し、不一致であれば(受信したトランザクション識別ビット反転していれば)、以前の中断されたトランザクションにおけるユーザ端末3のトランザクション処理が完了したと判断し、さらに、受信したトランザクション識別ビットT(1)を保持する。これにより、コンテンツ配信装置1内に保持しているトランザクション識別ビットTも更新される。

同様に、コマンド通信フェーズP3aにおいて、コンテンツ配信装置1は、要求メッセージと共に受信したトランザクション識別ビットT( $=0$ )と保持している初期値T( $=1$ )とを比較し、不一致であれば(受信したトランザクション識別ビット反転していれば)、初回コマンド通信フェーズP2におけるユーザ端末3のトランザクション処理が完了した

と判断し、さらに、受信したトランザクション識別ビット  $T (= 0)$  を保持する。これにより、コンテンツ配信装置 1 内に保持しているトランザクション識別ビット  $T$  も更新される。これ以降、コマンド通信フェーズが連続する場合も、同様である。

- 5      最後のコマンド通信フェーズの完了後、ユーザ端末 3 からコンテンツ配信装置 1 にコミットメッセージが送信される。これによりコミットフェーズ  $P 4$  が開始する。コンテンツ配信装置 1 はコミットメッセージを受信したとき、保持しているトランザクション識別ビット  $T$  を削除する。ユーザ端末 3 は、コミットメッセージに対する応答メッセージを受信したとき、トランザクション識別ビット  $T$  を削除する。このようにして、連続するトランザクション処理が 1 つのセッション上で行われる。

図 10 C は、コンテンツ配信装置 1 とユーザ端末 3 との間で複数のトランザクション処理が正常に実行されなかった場合のトランザクション識別ビットの遷移を示す説明図である。同図では、初回コマンド通信フェーズ  $P 2$  において、コンテンツ配信装置 1 が送信した応答メッセージを、通信切断等の理由によりユーザ端末 3 が正常に受信できなかった場合を示している。

ユーザ端末 3 は、正常に応答メッセージを受信できなかった場合、中断しているトランザクションを再開するために、再度初期フェーズから通信を再開させる。

同図の初期フェーズ  $P 1 1$  の開始時点で、コンテンツ配信装置 1 およびユーザ端末 3 はそれぞれトランザクション識別ビット  $T = 1$  になっている。初期フェーズ  $P 1 1$  において、認証情報  $A$  を受信したコンテンツ配信装置 1 は、内部にトランザクション識別ビット  $T (= 1)$  が保存されているので、そのトランザクション識別ビット  $T (= 1)$  と認証情報  $B$  とをユーザ端末 3 に送信する。これを受信したユーザ端末 3 は、受信

したトランザクション識別ビット  $T (= 1)$  と保持しているトランザクション識別ビット  $T (= 1)$  とが一致していることから、中断しているトランザクションにおいて前に送信した要求メッセージがコンテンツ配信装置 1 に届いたけれども、その応答メッセージがユーザ端末 3 に届かなかったと判断する。この場合、前に送信した要求メッセージが届いているので、コンテンツ配信装置 1 もトランザクションが中断された状態にあると判断している。また、ユーザ端末 3 は、前回のトランザクションが中断しているので受信したトランザクション識別ビットを反転することなく保存する。

10 次の初回コマンド通信フェーズ  $P 1 2$  において、ユーザ端末 3 は前に送信した要求メッセージと同じ内容の要求メッセージをトランザクション識別ビット  $T (= 1)$  と共に再度送信する。これを受信したコンテンツ配信装置 1 は、受信したトランザクション識別ビット  $T (= 1)$  と内部に保持しているトランザクション識別ビット  $T (= 1)$  が一致することから、中断したトランザクションの再開トランザクションであると判断する。この場合、トランザクションが未完了なので、コンテンツ配信装置 1 は内部に保存しているトランザクション識別ビットを反転しない。さらに、コンテンツ配信装置 1 は、要求メッセージに対応する応答メッセージを再度送信することになる。

20 これ以降のコマンド通信フェーズについては図 10B と同様である。

図 10D は、コンテンツ配信装置 1 とユーザ端末 3 との間でトランザクション処理が正常に実行されなかった場合のトランザクション識別ビットの遷移を示す説明図である。同図では、図 10C と異なり、初回コマンド通信フェーズ  $P 2$  において、応答メッセージの前の要求メッセージをコンテンツ配信装置 1 が正常に受信できなかった場合を示している。

ユーザ端末 3 は、正常に応答メッセージを受信できなかった場合、中

断しているトランザクションを再開するために、再度初期フェーズから通信を再開させる。

同図の初期フェーズ P 1 2 の開始時点で、コンテンツ配信装置 1 およびユーザ端末 3 はそれぞれトランザクション識別ビット  $T = 0$ 、 $T = 1$  になっている。初期フェーズ P 1 2 において、認証情報 A を受信したコンテンツ配信装置 1 は、内部にトランザクション識別ビット  $T (= 0)$  が保存されているので、そのトランザクション識別ビット  $T (= 0)$  と認証情報 B とをユーザ端末 3 に送信する。これを受信したユーザ端末 3 は、受信したトランザクション識別ビット  $T (= 0)$  と保持しているトランザクション識別ビット  $T (= 1)$  とが不一致であることから、中断しているトランザクションにおいて前に送信した要求メッセージがコンテンツ配信装置 1 にまで届かなかったと判断する。この場合、前に送信した要求メッセージが届いていないので、コンテンツ配信装置 1 はトランザクションが中断された状態にあると判断していない。これに対してユーザ端末 3 はトランザクションの中断原因が要求メッセージの不達であると判断することができる。また、ユーザ端末 3 は、前回のトランザクションが中断しているので受信したトランザクション識別ビットを反転することなく保存する。

次の初回コマンド通信フェーズ P 1 2 において、ユーザ端末 3 は前に送信した要求メッセージと同じ内容の要求メッセージをトランザクション識別ビット  $T (= 1)$  と共に再度送信してもよいし、新たな要求メッセージを送信してもよい。なぜなら、ユーザ端末 3 は、トランザクションの中断原因が要求メッセージの不達であると判断しているからである。つまり、コンテンツ配信装置 1 では、どの要求メッセージに対しても新規トランザクションと扱われるからである。ユーザ端末 3 からの要求メッセージが再送または新規メッセージが送信されると、コンテンツ配信

装置 1 は、受信したトランザクション識別ビット  $T (= 1)$  と保持しているトランザクション識別ビット  $T (= 0)$  とが一致しないことから新たなトランザクションと判断し、受信したトランザクション識別ビット  $T (= 1)$  を保存する（反転することになる）。さらに、コンテンツ配信

5 装置 1 は、要求メッセージに応じた応答メッセージを送信する。

これ以降の通信フェーズについては図 10B と同様である。

次に、図 11 ～ 図 15 を参照して、上述したコンテンツ利用処理において、コンテンツの利用要求（図 9 のステップ S 9 1）、および、利用権利とコンテンツの送信（図 9 のステップ S 9 4、S 9 5）が複数回行われる際の、各フェーズでの処理を説明する。

図 11 は、コンテンツ利用処理におけるユーザ端末 3 とコンテンツ配信装置 1 との初期フェーズで行われる処理について記述している。図 12 は、初期フェーズ後、初回コマンド通信フェーズを開始する前にユーザ端末 3 において行われる処理について記述している。図 13 は初回コマンド通信フェーズで行われる処理について記述している。図 14 はコマンド通信フェーズで行われる処理について記述している。さらに、図 15 はコミットフェーズで行われる処理について記述している。

まず、図 11 を参照して、ユーザ端末 3 とコンテンツ配信装置 1 との初期フェーズで行われる処理について説明する。ユーザ端末 3 のセキュリティ管理／通信部 36 に含まれる制御部 304 は、ユーザ指示処理部 31 からコンテンツ利用要求の送信を指示された場合、乱数発生部 302 で生成した乱数  $R_c$  と、固有情報記憶部 301 に記憶している端末公開鍵証明書を、通信部 305 を介して、コンテンツ配信装置 1 へ送信する（ステップ S 1101）。

25 コンテンツ配信装置 1 のセキュリティ管理／通信部 17 に含まれる制御部 204 は、通信部 205 を介してユーザ端末 3 から、乱数  $R_c$ 、端

末公開鍵証明書を受信すると、まず、固有情報記憶部201に記憶している認証局公開鍵証明書と、前記端末公開鍵証明書とを、暗号処理部203に与えることにより、前記端末公開鍵証明書の署名検証を行う（ステップS1102）。

- 5      上記ステップS1102における署名検証の結果、検証失敗となった場合（ステップS1103, No）、制御部204は、要求を拒絶する旨を、通信部205を介してユーザ端末3へ通知する（ステップS1104）。

- 10      一方、上記ステップS1102における署名検証の結果、検証が成功した場合（ステップS1103, Yes）、制御部204は、乱数発生部202で乱数Rs、Rs2を生成し、暗号処理部203で、乱数Rs2を入力としてDiffie-HellmanパラメータDHsの生成を行う（ステップS1105）。

- 15      さらに、制御部204は、通信ログデータベース206を検索し、トランザクション識別ビットが保存されているかを調べる。その結果、トランザクション識別ビットが保存されていない場合（つまり前回のコミットフェーズで削除され正常に終了した場合）は、トランザクション識別ビットTを初期値0とし、そうでない場合は、トランザクション識別ビットTを保存されているトランザクション識別ビットの値に設定する。
- 20      その後、ユーザ端末3から受信した乱数Rc、トランザクション識別ビットT、ステップS1105で生成したDHsを連結したデータ（式1）の署名（式2）を暗号処理部203で生成する（ステップS1106）。ここで、トランザクション識別ビットTは、この初期フェーズに続く初期コマンド通信フェーズで処理されるコンテンツ要求トランザクション
- 25      に対応付けられたビットであり、今後、通信切断が発生した場合には、このトランザクション識別ビットTを用いて、中断されたトランザクシ

ヨンの再開が行われる。

$$R_c || T || DH_s \quad (式 1)$$

$$S(s, R_c || T || DH_s) \quad (式 2)$$

制御部 204 は、ステップ S 1105 で生成した乱数  $R_s$  および  $Diffie-Hellman$  パラメータ  $DH_s$  と、トランザクション識別ビット  $T$  と、固有鍵情報記憶部 201 に記憶しているサーバ公開鍵証明書と、ステップ S 1106 で生成した署名（式 2）をユーザ端末 3 に通信部 205 を介して送信する（ステップ S 1107）。

次に、図 12 を参照して、初期フェーズ後、初回コマンド通信フェーズを開始する前にユーザ端末 3 において行われる処理について説明する。

ユーザ端末 3 のセキュリティ管理／通信部 36 に含まれる制御部 304 は、通信部 305 を介してコンテンツ配信装置 1 から、乱数  $R_s$ 、トランザクション識別ビット  $T$ 、 $Diffie-Hellman$  パラメータ  $DH_s$ 、サーバ公開鍵証明書、および署名データを受信すると、まず、固有情報記憶部 301 に記憶している認証局公開鍵証明書と、前記サーバ公開鍵証明書とを、暗号処理部 303 に与えることにより、前記サーバ公開鍵証明書の署名検証を行う（ステップ S 1201）。

上記ステップ S 1201 における署名検証の結果、検証失敗となった場合（ステップ S 1202, No）、制御部 304 は、コンテンツ利用要求を拒絶する旨を、ユーザ指示処理部 31 へ通知する（ステップ S 1203）。

一方、上記ステップ S 1201 における署名検証の結果、検証が成功した場合（ステップ S 1202, Yes）、制御部 304 は、ステップ S 1101 で作成した乱数  $R_c$  とステップ S 1107 でコンテンツ配信装置 1 から受信したトランザクション識別ビット  $T$ 、および  $DH_s$  を結合したデータ（式 3）を生成し、そのデータ（式 3）、ステップ S 1107

でコンテンツ配信装置 1 から受信した署名データ（式 2）、およびサーバ公開鍵証明書を暗号処理部 303 に入力し、署名データ（式 2）の検証を行う（ステップ S 1204）。

$$R_c || T || DH_s \quad (式 3)$$

- 5      上記ステップ S 1204 における署名検証の結果、検証失敗となった場合（ステップ S 1205, No）、制御部 304 は、コンテンツ利用要求を拒絶する旨を、ユーザ指示処理部 31 へ通知する（ステップ S 1203）。

- 一方、上記ステップ S 1204 における署名検証の結果、検証が成功  
10    した場合（ステップ S 1205, Yes）、ユーザ端末 3 は通信相手が確かにコンテンツ配信装置 1 であることが分かる（通信相手の認証）。制御部 304 は、乱数発生部 302 で乱数  $R_c2$  を生成し、生成した乱数  $R_c2$  を暗号処理部 303 の入力として Diffie-Hellman パラメータ  $DH_c$  を生成する（ステップ S 1206）。

- 15      さらに、制御部 304 は、ステップ S 1107 でコンテンツ配信装置 1 から受信した  $DH_s$  と、ステップ S 1206 で生成した  $R_c2$  とから、暗号処理部 303 でセッション鍵  $KS$  を生成する（ステップ S 1207）。

- その後、制御部 304 は、ステップ S 1107 でコンテンツ配信装置 1 から受信したトランザクション識別ビット  $T$  を通信ログデータベース  
20    306 に記憶する（ステップ S 1208）。これにより、トランザクション通信ビット  $T$  に対応するコンテンツ利用要求トランザクションが開始され、レスポンス待ち状態であることがデータベースに保存される。

- 制御部 304 は、ステップ S 1107 でコンテンツ配信装置 1 から受信した乱数  $R_s$  とステップ S 1206 で生成した  $DH_c$  を連結したデータ  
25    （式 4）の署名（式 5）を暗号処理部 303 で生成し、ステップ S 1207 で生成したセッション鍵  $KS$  で、ステップ S 1108 で保存した



トランザクション識別ビットを反転し、反転したトランザクション識別  
ビットTとコンテンツ利用要求メッセージMを暗号化する（ステップS  
1209）。コンテンツ利用要求メッセージは、少なくとも利用するコン  
テンツのコンテンツ識別子を含む。暗号化データにはシーケンス番号S  
5 e qとハッシュ値hを付加する（式6）。ハッシュの対象データはシーケ  
ンス番号S e qとコンテンツ利用要求メッセージMとする。シーケンス  
番号は、セッションが開始されたとき、つまり、初期フェーズが開始さ  
れる際に0にリセットされ、メッセージの送信および受信の度に1ずつ  
加算される通し番号である。

10 
$$R s \parallel D H c \quad (\text{式 } 4)$$

$$S(c, R s \parallel D H c) \quad (\text{式 } 5)$$

$$E(K S, S e q \parallel T \parallel M \parallel h) \quad (\text{式 } 6)$$

制御部304は、ステップS1206で生成したDHcと、ステップ  
S1209で生成した署名（式5）と暗号化データ（式6）をコンテン  
15 ツ配信装置1に通信部305を介して送信する（ステップS1210）。

次に、図13を参照して、初回コマンド通信フェーズで行われる処理  
について説明する。

コンテンツ配信装置1のセキュリティ管理／通信部17に含まれる制  
御部204は、通信部205を介してユーザ端末3から、D i f f i e  
20 - H e l l m a nパラメータDHc、署名データ、および暗号化データ  
を受信すると、ステップS1105で作成した乱数RsとステップS1  
210でユーザ端末3から受信したDHcを結合したデータ（式7）を  
生成し、その生成データ（式7）、ステップS1210でユーザ端末3か  
ら受信した署名データ、および端末公開鍵証明書を暗号処理部203に  
25 入力し、署名データの検証を行う（ステップS1301）。

$$R s \parallel D H c \quad (\text{式 } 7)$$

上記ステップS 1 3 0 1における署名検証の結果、検証失敗となった場合（ステップS 1 3 0 2, N o）、制御部2 0 4は、コンテンツ利用要求を拒絶する旨を、通信部2 0 5を介してユーザ端末3へ通知する（ステップS 1 3 0 3）。

5 一方、上記ステップS 1 3 0 1における署名検証の結果、検証が成功した場合（ステップS 1 3 0 2, Y e s）、コンテンツ配信装置1は通信相手が確かにユーザ端末3であることが分かる（通信相手の認証）。制御部2 0 4は、ステップS 1 2 1 0でユーザ端末3から受信したD H cと、ステップS 1 1 0 5で生成したR s 2とから、暗号処理部2 0 3でセッション鍵K Sを生成する。その後、ステップ1 2 1 0で受信した暗号化データと生成したK Sを暗号処理部2 0 3に入力し暗号化データの復号を行い、シーケンス番号とハッシュ値のチェックを行う（ステップS 1 3 0 4）。

さらに、制御部2 0 4は、通信ログデータベースを検索し、トランザク  
15 クション識別ビットを取得する。その結果、トランザクション識別ビットが存在しない、もしくは、その値がステップS 1 2 1 0で受信したトランザクション識別ビットTと一致しない場合（ステップS 1 3 0 5, N o）、コンテンツ配信装置1は、要求メッセージが新規のトランザクションのものと判断し、制御部2 0 4は、ステップS 1 3 0 1でユーザ端  
20 末3から受信したトランザクション識別ビットTを通信ログデータベース2 0 6に記憶する（ステップS 1 3 0 6）。これにより、トランザクション識別ビットTが反転することになる。また、コンテンツ利用要求トランザクションが、このステップまで完了したことがデータベースに保存される。

25 その後、制御部2 0 4はユーザ権利生成部1 4に新規トランザクションとして、ステップS 1 2 1 0でユーザ端末3から受信したコンテンツ

利用要求を通知する（ステップS 1 3 0 7）。

一方、トランザクション識別ビットが既に存在し、その値がステップ  
S 1 2 1 0 で受信したトランザクション識別ビットTと一致した場合  
（ステップS 1 3 0 5, Y e s）、制御部2 0 4は、通信切断などのより  
5 トランザクションが中断されたと判断し、ユーザ権利生成部1 4に再開  
トランザクションとして、ステップS 1 2 1 0でユーザ端末3から受信  
したコンテンツ利用要求を通知する（ステップS 1 3 0 8）。

制御部2 0 4は、シーケンス番号とユーザ権利作成部1 4で作成され  
た利用権利とそれらのハッシュ値をステップS 1 3 0 4で生成したセッ  
10 ション鍵KSを用いて暗号処理部2 0 3で暗号化して、通信部2 0 5を  
介してユーザ端末3に送信する（ステップS 1 3 0 9）。ここで、送信さ  
れる利用権利は、コンテンツ配信装置1とユーザ端末3のみで生成可能  
なセッション鍵KSで暗号化されているため、第三者が盗聴することは  
できない。

15 ユーザ端末3のセキュリティ管理／通信部3 6に含まれる制御部3 0  
4は、通信部3 0 5を介してコンテンツ配信装置1から、暗号化データ  
を受信すると、まず、暗号処理部3 0 3でセッション鍵KSを用いて暗  
号化データの復号を行い、シーケンス番号、利用権利、ハッシュ値を復  
元する。その後、シーケンス番号とハッシュ値のチェックを行い、利用  
20 条件をユーザ指示処理部3 1へ通知する。さらに、通信ログデータベ  
ース3 0 6に保存しているトランザクション識別ビットを反転させる。（ス  
テップS 1 3 1 0）。これにより、トランザクション識別ビットTに対応  
するトランザクションが完了したこととなる。

この後、引き続きトランザクションがある場合にはステップS 1 4 0  
25 1へ、そうでない場合はステップS 1 5 0 1へ移る。

次に、図1 4を参照して、コマンド通信フェーズで行われる処理につ

いて説明する。

制御部 304 は、初期化フェーズで生成したセッション鍵  $K_S$  で、通信ログデータベース 306 に記憶するトランザクション識別ビット  $T$  とコンテンツ利用要求メッセージ  $M$  を暗号化する（ステップ  $S1401$ ）。

- 5 コンテンツ利用要求メッセージは、少なくとも利用するコンテンツのコンテンツ識別子を含む。暗号化データにはシーケンス番号  $S_{eq}$  とハッシュ値  $h$  を付加する。ハッシュの対象データはシーケンス番号  $S_{eq}$  とコンテンツ利用要求メッセージ  $M$  とする。

- 10 制御部 304 は、ステップ  $S1401$  で生成した暗号化データをコンテンツ配信装置 1 に通信部 305 を介して送信する（ステップ  $S1402$ ）。

- コンテンツ配信装置 1 のセキュリティ管理／通信部 17 に含まれる制御部 204 は、通信部 205 を介してユーザ端末 3 から暗号化データを受信すると、暗号化データと初回コマンド通信フェーズで生成した生成した  $K_S$  を暗号処理部 203 に入力し暗号化データの復号を行い、シーケンス番号とハッシュ値のチェックを行う（ステップ  $S1403$ ）。
- 15

- さらに、制御部 204 は、通信ログデータベースを検索し、ステップ  $S1402$  でユーザ端末 3 から受信したトランザクション識別ビット  $T$  と通信ログデータベースに保持するトランザクション識別ビットと一致するかを調べる。その結果、一致しない場合（ステップ  $S1404$ 、 $No$ ）、制御部 204 は、ステップ  $S1402$  でユーザ端末 3 から受信した  $T$  に通信ログデータベース 206 の内容を変更する（ステップ  $S1405$ ）。これにより、トランザクション識別ビット  $T$  が反転することになる。また、コンテンツ利用要求トランザクションが、このステップまで完了したことがデータベースに保存される。
- 20
- 25

その後、制御部 204 はユーザ権利生成部 14 に新規トランザクショ

ンとして、ステップS 1 4 0 2でユーザ端末3から受信したコンテンツ利用要求を通知する（ステップS 1 4 0 6）。

一方、トランザクション識別ビットTが通信ログデータベース2 0 6に保持するトランザクション識別ビットと一致する場合（ステップS 1 4 0 4, Y e s）、制御部2 0 4は、通信切断等によりトランザクションが中断されたものと判断し、ユーザ権利生成部1 4に再開トランザクションとして、ステップS 1 4 0 2でユーザ端末3から受信したコンテンツ利用要求を通知する（ステップS 1 4 0 7）。

制御部2 0 4は、シーケンス番号とユーザ権利作成部1 4で作成された利用権利とそれらのハッシュ値を初回コマンド通信フェーズで生成したセッション鍵K Sを用いて暗号処理部2 0 3で暗号化して、通信部2 0 5を介してユーザ端末3に送信する（ステップS 1 4 0 8）。ここで、送信される利用権利は、コンテンツ配信装置1とユーザ端末3のみで生成可能なセッション鍵K Sで暗号化されているため、第三者が盗聴することはできない。

ユーザ端末3のセキュリティ管理／通信部3 6に含まれる制御部3 0 4は、通信部3 0 5を介してコンテンツ配信装置1から、暗号化データを受信すると、まず、暗号処理部3 0 3でセッション鍵K Sを用いて暗号化データの復号を行い、シーケンス番号、利用権利、ハッシュ値を復元する。その後、シーケンス番号とハッシュ値のチェックを行い、利用条件をユーザ指示処理部3 1へ通知する。さらに、通信ログデータベース3 0 6に保存しているトランザクション識別ビットTを反転する。（ステップS 1 4 0 9）。これにより、トランザクション識別ビットTに対応するトランザクションが完了したこととなる。

この後、引き続きトランザクションがある場合にはステップS 1 4 0 1へ、そうでない場合はステップS 1 5 0 1へ移る。

最後に、図 15 を参照して、コミットフェーズで行われる処理を説明する。

制御部 304 は、初期化フェーズで生成したセッション鍵 K S で、コミットメッセージを暗号化する（ステップ S 1501）。

- 5     制御部 304 は、ステップ S 1501 で生成した暗号化データをコンテンツ配信装置 1 に通信部 305 を介して送信する（ステップ S 1502）。

- 10     コンテンツ配信装置 1 のセキュリティ管理／通信部 17 に含まれる制御部 204 は、通信部 205 を介してユーザ端末 3 から暗号化データを受信すると、暗号化データと初回コマンド通信フェーズで生成した生成した K S を暗号処理部 203 に入力し暗号化データの復号を行う（ステップ S 1503）。

さらに、制御部 204 は、通信ログデータベース 206 に記憶しているトランザクション識別ビットを削除する（ステップ S 1504）。

- 15     制御部 204 は、ACK メッセージを初回コマンド通信フェーズで生成したセッション鍵 K S を用いて暗号処理部 203 で暗号化して、通信部 205 を介してユーザ端末 3 に送信する（ステップ S 1505）。

- 20     ユーザ端末 3 のセキュリティ管理／通信部 36 に含まれる制御部 304 は、通信部 305 を介してコンテンツ配信装置 1 から、暗号化データを受信すると、まず、暗号処理部 303 でセッション鍵 K S を用いて暗号化データの復号を行い、ACK メッセージを復元し、コミット処理が完了したことをユーザ指示処理部 31 へ通知する。その後、通信ログデータベース 306 に保存しているトランザクション識別ビット T を削除する。（ステップ S 1506）。

- 25     なお、通信切断後のトランザクション再開処理は、ユーザ指示処理部 31 からのトランザクション再開処理要求によって開始され、初期フェ

ーズを処理した後、通信切断により中断されているトランザクションに対応するトランザクション識別ビット（通信ログデータベースに保存されているトランザクション識別ビット）Tを用いて、初回コマンド通信フェーズによって再開される。この初回コマンド通信フェーズで送信されるコンテンツ利用要求メッセージは、ユーザ指示処理部31が再度、制御部304に渡してもよいし、制御部304が通信ログデータベースにトランザクション識別ビットを保存する際にコンテンツ利用要求メッセージも保存するようにし、その保存しておいたメッセージを利用してもよい。

10 上記処理により、ユーザ端末3の認証処理、利用権利の盗聴・改ざん防止処理、および通信切断対策処理を行うことが可能となる。

本実施の形態で示した通信プロトコルにおいて、n個のトランザクションを処理する際の通信往復回数は、初期フェーズで1往復、初回コマンド通信フェーズで1往復、コマンド通信フェーズでn-1往復、コミットフェーズで1往復となり、合計n+2回となる。

15 なお、本実施の形態で用いた暗号アルゴリズム、セッション鍵共有アルゴリズム、証明書フォーマットなどは、同等の機能を持つものであれば、必ずしも記載したものを用いる必要はない。例えば、データの暗号アルゴリズムにはTriple DESを用いてもよい。また、暗号化データに付与されるハッシュ値は、CRCなどのチェックサム値を用いてもよい。さらに、SACプロトコルには公開鍵暗号方式の代わりに共通鍵暗号方式を用いてもよい。

20 なお、本実施の形態では、ユーザ端末3からの端末公開鍵証明書は、初期化フェーズ（図11のステップS1101）において送信したが、初回コマンド通信フェーズ（図12のステップS1210）において送信してもよい。これにより、コンテンツ配信装置1は、装置内に上記デ

ータを保持しておく必要がなくなる。この場合、コンテンツ配信装置 1  
での端末公開鍵証明書の署名検証処理（図 1 1 のステップ S 1 1 0 2）  
は、初回コマンド通信フェーズの最初（図 1 3 のステップ S 1 3 0 1 の  
直前）で行うこととなる。

5      なお、ステップ S 1 1 0 7 において、コンテンツ配信装置 1 からユー  
ザ端末 3 へ送信されるデータに、ユーザ端末 3 から受信した乱数  $R_c$  を  
含めてもよい。つまり、コンテンツ配信装置 1 から送信されるデータは、  
乱数  $R_c$ 、乱数  $R_s$ 、トランザクション識別ビット  $T$ 、パラメータ  $DH_s$   
、署名データとなる。これにより、ユーザ端末 3 は、乱数  $R_c$  を端末  
10   内に保持しておく必要がなくなる。同様に、ステップ S 1 2 1 0 におい  
て、ユーザ端末 3 からコンテンツ配信装置 1 へ送信されるデータに、コ  
ンテンツ配信装置 1 から受信した乱数  $R_s$  を含めてもよい。つまり、コ  
ンテンツ配信装置 1 から送信されるデータは、乱数  $R_s$ 、パラメータ  $DH_c$   
、署名データ、暗号化データとなる。

15      なお、本実施の形態においては、ユーザ端末 3 がコンテンツ配信装置  
1 を認証する処理も含まれているが、特に必要がない場合には、認証処  
理を除いてもよい。

        なお、本実施の形態においては、コマンド通信フェーズでトランザク  
ション識別ビットの一致判定を行っているが、特に必要が無い場合には、  
20   判定処理を除いてもよい。この場合、コマンド通信フェーズで処理され  
るトランザクションは常に新規トランザクションとして処理される。

        なお、本実施の形態においては、トランザクション識別ビットをコン  
テンツ配信装置 1 から送信するようにしているが、これを省略してもよ  
い。つまり、初期フェーズにおけるコンテンツ配信装置 1 の処理および、  
25   初期フェーズにおけるメッセージ中のトランザクション識別ビットに関  
する情報は省略される。



5      なお、本実施の形態においては、ステップ S 1 3 0 8 およびステップ  
S 1 4 0 7 においてユーザ権利の作成を行う際に、セキュリティ管理／  
通信部 1 7 から再開トランザクションとして指示された場合には、登録  
内容の更新を行わないとしたが、再度、コンテンツ利用要求を評価し、  
10    ユーザ権利の作成をやり直してもよい。これにより、新規トランザクシ  
ョンの発行と再開トランザクションの発行の間に起こった状況変化に対  
応することが可能となる。例を挙げれば、新規トランザクション発行時  
には、コンテンツの利用有効期限内であったので利用権利の作成・送信  
を行ったが、再開トランザクションとして再度要求が行われたときには、  
10    コンテンツの利用有効期限を越えたい場合が考えられる。この場合に  
は、再開トランザクションに対しては利用権利の作成・発行は行わない。

15    また、本実施の形態においては、通信切断によって処理途中のラン  
ザクションのキャンセル処理を含めてもよい。キャンセル処理を行う場  
合、通信切断後の初回コマンド通信フェーズで、レスポンスをまだ受信  
していないトランザクションに対応するトランザクション識別ビット T  
（通信ログデータベース 3 0 6 に保存しているもの）を含むキャンセル  
メッセージをユーザ指示処理部 3 1 の指示によりユーザ端末 3 から送信  
20    する。キャンセルメッセージを受信したコンテンツ配信装置 1 は、ユー  
ザ権利作成部 1 4 にその旨を通知し、処理途中のトランザクションを処  
理前の状態にロールバックさせる。その後、コンテンツ配信装置 1 はユ  
ーザ端末 3 に対して、ACKメッセージを送信する。

25    また、コンテンツ配信装置 1 とユーザ端末 3 との間の 2 つのコンテン  
ツ利用要求処理を処理 A および処理 B とするとき、処理 A の終了後に、  
一旦、通信切断を行わなければならない場合、通常は、処理 B の開始時  
には再度認証処理を行い、新たなセッション鍵を作成し直すが、処理 B  
の応答時間を削減したい場合には、処理 B での認証処理を除くために、

処理 A でのセッション鍵をコンテンツ配信装置 1 とユーザ端末 3 の双方で記憶しておき、再利用してもよい。

5       なお、本実施の形態においては、コンテンツ配信装置 1 はセッション鍵の利用制限を設けてもよい。例えば、セッション鍵の再利用回数が規定の上限を超えた場合、セッション鍵が最初に作成されたから規定の時間が経過した場合、セッション鍵が最初に作成されてから規定の通信データ量を超えた場合、予め決められたコンテンツあるいは利用権利を配信する場合、あるいは、予め決められたユーザ端末 3 に配信する場合などに、コンテンツ配信装置 1 はユーザ端末 3 にセッション鍵再利用不可  
10      通知を行う。セッション鍵再利用不可通知を受信したユーザ端末 3 は、セッション鍵を生成しなおす。つまり、初期フェーズから通信をやり直す。

      なお、本実施の形態においては、コンテンツ配信装置 1 とユーザ端末 3 との間のプロトコルとして説明を行ったが、ユーザ端末同士でのライセンス交換にも適用可能である。例えば、家庭内のユーザ端末同士でラ  
15      イセンスを移動させる場合に適用できる。その際、同一家庭内のユーザ端末であるというグループ識別子が予め、あるいは、購入後の設定により指定されているものとする。ユーザ端末間でライセンスを移動させる際に本実施の形態で示したプロトコルを適用する場合、ライセンスの移動元端末をコンテンツ配信装置 1 に、ライセンスの移動先端末をユーザ  
20      端末 3 と捉えればよい。なお、ライセンスの移動を同一家庭内、つまり、同一グループ識別子を持つもの同士に限る場合には、ライセンス配信先端末からライセンス配信元端末にグループ識別子を送信し、ライセンス配信元端末が同一グループ識別子かどうかを判定し、同一である場合のみ  
25      ライセンスの送信を行うようにする。グループ識別子の送信は、盗聴・改ざん・成りすましを防ぐ方法であれば、どのような方法であってもよ

い。例えば、初回コマンド通信フェーズの暗号化データに含めてもよい。  
また、グループ識別子そのものを送信せず、グループ識別子のハッシュ  
値を用いてもよい。さらに、別途、グループ識別子ハッシュ送信フェー  
ズを初期フェーズの後に設けて、セッション鍵で暗号化したグループ識  
5 別子ハッシュを送信してもよい。

なお、本実施の形態で示したコンテンツ配信システムの各構成要素は、  
ハードウェアで実現しても、ソフトウェアで実現してもよい。

以上のように本発明によれば、ライセンスの盗聴・改ざんの防止、通信  
相手の認証、通信切断対策のすべての機能を実現するとともに、複数ト  
10 ランザクション処理を行う場合においても、サーバ装置・端末装置間の  
通信往復回数を減少させ、さらに、上記機能を実現するためにサーバ装  
置と端末装置で管理・保持する情報が少ないプロトコルを実現するシス  
テムおよび装置を提供する。これにより、ユーザが要求を出してから、  
応答を得るまでの待ち時間を短縮させることが可能なコンテンツ配信シ  
15 ステムを提供することができる。

#### 産業上の利用可能性

本発明は、要求メッセージの受信、応答メッセージの送信、トランザ  
クション完了を確定させるためのコミットメッセージの受信を含むトラ  
20 ンザクション処理に基づいて端末装置にコンテンツの利用に対するライ  
センスを提供するサーバ装置と、前記サーバ装置から取得した前記ライ  
センスに基づいて前記コンテンツの利用を制御する端末装置とを含むデ  
ジタルコンテンツ配信システムに適している。例えば、サーバ装置とし  
ては、インターネットを介してデジタルコンテンツを配信するサービス  
25 プロバイダの配信サーバや、放送を介してデジタルコンテンツをデジタ  
ル放送する放送装置等に適しており、端末装置としては、デジタル放送

を受信するためのセットトップボックス、デジタルＴＶ、ＤＶＤレコーダ、ハードディスクレコーダ、パーソナルコンピュータなどのコンテンツ再生装置、記録装置あるいはこれらの複合機器等に適している。

## 請 求 の 範 囲

1. 要求メッセージの送信、応答メッセージの受信、1つのトランザクション完了を確定させるためのコミットメッセージの送信を含むトランザクション処理に基づいてサーバ装置からコンテンツの利用に対するライセンスを取得し、前記ライセンスに基づいて前記コンテンツの利用を制御する端末装置であって、

- 現在のトランザクション処理について処理中であるか処理済みであることを示す1ビットのトランザクション識別フラグを保持する保持手段と、  
連続する複数回のトランザクション処理における最終回を除く各トランザクション処理においてコミットメッセージを送信しないで、2回目以降の要求メッセージの送信時に、コミットメッセージの代わりに前記トランザクション識別ビットを送信する送信手段と  
を備えることを特徴とする端末装置。

2. 前記端末装置は、

- 前記複数のトランザクション処理においてサーバ装置から送信される各応答メッセージを受信する応答受信手段と、  
応答受信手段による受信結果に従って、前記保持手段に保持されたトランザクション識別フラグを更新する更新手段と  
を備えることを特徴とする請求の範囲第1項に記載の端末装置。

3. 前記更新手段は、

- 前記サーバ装置に保持されるトランザクション識別フラグと同じ値を、保持手段に保持されるトランザクション識別フラグの初期値として設定し、

応答受信手段によって応答メッセージが受信されたとき、保持手段の

トランザクション識別フラグの値を反転する

ことを特徴とする請求の範囲第2項に記載の端末装置。

4. 前記トランザクション識別フラグの初期値は、前記複数のトランザクション処理においてサーバ装置から送信される初回の応答メッセージに含まれ、

前記更新手段は、

応答受信手段によって初回の応答メッセージが受信されたとき、保持手段のトランザクション識別フラグを初期値に設定し、

- 10 応答受信手段によって応答メッセージが正常に受信されたとき、保持手段のトランザクション識別フラグの値を反転する

ことを特徴とする請求の範囲第3項に記載の端末装置。

5. 前記送信手段は、

- 15 前記複数のトランザクション処理において、2回目以降の要求メッセージの送信時に、コミットメッセージ送信の代用として前記トランザクション識別ビットを送信する要求送信手段と、

前記複数トランザクション処理中の最後のトランザクション処理においてのみコミットメッセージを送信するコミット送信手段と

- 20 を備えることを特徴とする請求の範囲第3項に記載の端末装置。

6. 前記要求送信手段は、

前記信応答受信手段によって応答メッセージが正常に受信されたとき、更新手段により反転されたトランザクション識別ビットを、次のトラン

- 25 ザクション処理の要求メッセージとともに送信する

ことを特徴とする請求の範囲第5項に記載の端末装置。

7. 前記要求送信手段は、

前記応答受信手段によって応答メッセージが正常に受信されなかったとき、反転されていないトランザクション識別ビットを、現在のトランザクション処理の要求メッセージとともに再度送信する

ことを特徴とする請求の範囲第6項に記載の端末装置。

8. 前記端末装置は、複数のトランザクション処理における初回のトランザクション処理の直前にサーバ装置との間で相互認証する処理を行い、

前記端末装置は、さらに、

サーバ装置が端末装置を認証するための第1認証情報を認証要求として送信手段に提供し、

応答受信手段によって前記第1認証情報に対する応答として受信された、端末装置がサーバ装置を認証するため第2認証情報を検証し、

検証の結果、相互認証を確定させるための確定メッセージを送信手段に提供する認証手段を備え、

前記送信手段は、前記確定メッセージを、前記初回のトランザクション処理の要求メッセージと共に送信する

ことを特徴とする請求の範囲第2項に記載の端末装置。

9. 前記複数のトランザクション処理を相互認証がなされたセッションと同一のセッション上で行う

ことを特徴とする請求の範囲第8項に記載の端末装置。

10. 前記更新手段は、

前記サーバ装置に保持されるトランザクション識別フラグと同じ値を、

保持手段に保持されるトランザクション識別フラグの初期値として設定し、

応答受信手段によって応答メッセージが受信されたとき、保持手段のトランザクション識別フラグの値を反転する

5      ことを特徴とする請求の範囲第 8 項に記載の端末装置。

1 1 . 前記送信手段は、

前記複数のトランザクション処理において、2 回目以降の要求メッセージの送信時に、コミットメッセージ送信の代用として前記トランザク  
10      ション識別ビットを送信する要求送信手段と、

前記複数トランザクション処理中の最後のトランザクション処理においてのみコミットメッセージを送信するコミット送信手段と

を備えることを特徴とする請求の範囲第 1 0 項に記載の端末装置。

15      1 2 . 前記要求送信手段は、

前記信応答受信手段によって応答メッセージが正常に受信されたとき、更新手段により反転されたトランザクション識別ビットを、次のトランザクション処理の要求メッセージとともに送信する

ことを特徴とする請求の範囲第 1 1 項に記載の端末装置。

20

1 3 . 前記要求送信手段は、

前記信応答受信手段によって応答メッセージが正常に受信されなかったとき、反転されていないトランザクション識別ビットを、現在のトランザクション処理の要求メッセージとともに再度送信する

25      ことを特徴とする請求の範囲第 1 2 項に記載の端末装置。



14. 要求メッセージの受信、応答メッセージの送信、1つのトランザクション完了を確定させるためのコミットメッセージの受信を含むトランザクション処理に基づいて端末装置にコンテンツの利用に対するライセンスを提供するサーバ装置であって、

- 5 連続する複数回のトランザクション処理における2回目以降の要求メッセージと共に前記コミットメッセージの代わりに送信される1ビットのフラグであって、端末装置においてトランザクションを処理中であるか処理済みであることを示すトランザクション識別フラグを受信する受信手段と、
- 10 受信されたトランザクション識別フラグに基づいて1つのトランザクションの完了を確定するか否かを判定する判定手段と
- を備えることを特徴とするサーバ装置。

15. 前記トランザクション識別フラグは、端末装置によってトランザクションが処理される毎に反転された値を有し、

前記サーバ装置は、さらに、

前記複数のトランザクション処理における前回の要求メッセージと共に送信されたトランザクション識別フラグのコピーである第1フラグを保持する保持手段を備え、

- 20 前記判定手段は、

受信手段によって受信された現在のトランザクション処理におけるトランザクション識別フラグと、保持手段に保持された第1フラグとが不一致であるとき、前回のトランザクションの完了を確定すると判定することを特徴とする請求の範囲第14項に記載のサーバ装置。

25

16. 前記サーバ装置は、前記複数のトランザクション処理における初

回の応答メッセージとともに、第 1 フラグの初期値を前記トランザクション識別フラグの初期値として、端末装置に送信する応答送信手段を備える

ことを特徴とする請求の範囲第 15 項に記載のサーバ装置。

5

17. 前記受信手段は、

前記 2 回目以降の要求メッセージと共に前記トランザクション識別フラグを受信する要求受信手段と、

10 前記複数トランザクション処理中の最後のトランザクション処理においてのみコミットメッセージを受信するコミット受信手段と

を備えることを特徴とする請求の範囲第 15 項に記載のサーバ装置。

18. 前記応答送信手段は、

15 判定手段によって前回のトランザクションの完了を確定すると判定されたとき、次のトランザクション処理の応答メッセージを送信する

ことを特徴とする請求の範囲第 17 項に記載のサーバ装置。

19. 前記応答送信手段は、

20 判定手段によって前回のトランザクションの完了を確定しないと判定されたとき、前回のトランザクション処理の応答メッセージを再度送信する

ことを特徴とする請求の範囲第 18 項に記載のサーバ装置。

25 20. 前記サーバ装置は、前記複数のトランザクション処理中の初回のトランザクション処理の直前に端末装置との間で相互認証する処理を行い、

前記サーバ装置は、さらに、

受信手段によって認証要求として受信された、サーバ装置が端末装置を認証するための第1認証情報を検証し、

正当と検証されたとき、端末装置がサーバ装置を認証するため第2認証情報を提供する認証手段を備え、

前記要求受信手段は、前記初回の要求メッセージと共に、相互認証を確定させるための確定メッセージを受信する

ことを特徴とする請求の範囲第15項に記載のサーバ装置。

10 21. 前記複数のトランザクション処理を相互認証がなされたセッションと同一のセッション上で行う

ことを特徴とする請求の範囲第20項に記載のサーバ装置。

22. 前記受信手段は、

15 前記2回目以降の要求メッセージと共に前記トランザクション識別フラグを受信する要求受信手段と、

前記複数トランザクション処理中の最後のトランザクション処理においてのみコミットメッセージを受信するコミット受信手段と

を備えることを特徴とする請求の範囲第21項に記載のサーバ装置。

20

23. 前記応答送信手段は、

判定手段によって前回のトランザクションの完了を確定すると判定されたとき、次のトランザクション処理の応答メッセージを送信する

ことを特徴とする請求の範囲第22項に記載のサーバ装置。

25

24. 前記応答送信手段は、

判定手段によって前回のトランザクションの完了を確定しないと判定されたとき、前回のトランザクション処理の応答メッセージを再度送信する

ことを特徴とする請求の範囲第 2 3 項に記載のサーバ装置。

5

25. 要求メッセージの受信、応答メッセージの送信、トランザクション完了を確定させるためのコミットメッセージの受信を含むトランザクション処理に基づいて端末装置にコンテンツの利用に対するライセンスを提供するサーバ装置と、前記サーバ装置から取得した前記ライセンスに基づいて前記コンテンツの利用を制御する端末装置とを含むデジタルコンテンツ配信システムであって、

前記端末装置は、

現在のトランザクション処理について処理中であるか処理済みであるかを示す 1 ビットのトランザクション識別フラグを保持する保持手段と、

15 連続する複数回のトランザクション処理における最終回を除く各トランザクション処理においてコミットメッセージの送信を送信しないで、2 回目以降の要求メッセージの送信時に、コミットメッセージの代わりに前記トランザクション識別ビットを送信する送信手段とを備え、

前記サーバ装置は、

20 連続する複数回のトランザクション処理における 2 回目以降の要求メッセージと共に送信される前記トランザクション識別フラグを受信する受信手段と、

受信されたトランザクション識別フラグに基づいて 1 つのトランザクションの完了を確定するか否かを判定する判定手段とを備える

25 ことを特徴とするコンテンツ配信システム。

26. 要求メッセージの送信、応答メッセージの受信、1つのトランザクション完了を確定させるためのコミットメッセージの送信を含むトランザクション処理に基づいてサーバ装置からコンテンツの利用に対するライセンスを取得し、前記ライセンスに基づいて前記コンテンツの利用を制御する端末装置におけるトランザクション処理方法であって、

連続する複数回のトランザクション処理における最終回を除く各トランザクション処理においてコミットメッセージを送信しないで、2回目以降の要求メッセージの送信時に、コミットメッセージの代わりに、現在のトランザクション処理について処理中であるか処理済みであることを示す1ビットの前記トランザクション識別ビットを送信するよう制御する制御ステップと、

前記最終回のトランザクション処理においてコミットメッセージの送信する送信ステップと

を有することを特徴とするトランザクション処理方法。

15

27. 要求メッセージの受信、応答メッセージの送信、1つのトランザクション完了を確定させるためのコミットメッセージの受信を含むトランザクション処理に基づいて端末装置にコンテンツの利用に対するライセンスを提供するサーバ装置におけるトランザクション処理方法であって、

20

連続する複数回のトランザクション処理における2回目以降の要求メッセージと共に前記コミットメッセージの代わりに送信される1ビットのフラグであって、端末装置においてトランザクションを処理中であるか処理済みであることを示すトランザクション識別フラグを受信するステップと、

25

受信されたトランザクション識別フラグに基づいて1つのトランザク

ションの完了を確定するか否かを判定する判定ステップと

を有することを特徴とするトランザクション処理方法。

28. 要求メッセージの受信、応答メッセージの送信、トランザクシ  
5 ン完了を確定させるためのコミットメッセージの受信を含むトランザク  
ション処理に基づいて端末装置にコンテンツの利用に対するライセンス  
を提供するサーバ装置と、前記サーバ装置から取得した前記ライセンス  
に基づいて前記コンテンツの利用を制御する端末装置とを含むデジタル  
コンテンツ配信システムにおけるトランザクション処理方法であって、

10 前記端末装置において、連続する複数回のトランザクション処理にお  
ける最終回を除く各トランザクション処理においてコミットメッセージ  
を送信しないで、2回目以降の要求メッセージの送信時に、コミットメ  
ッセージの代わりに、現在のトランザクション処理について処理中であ  
るか処理済みであることを示す1ビットの前記トランザクション識別ビッ  
15 トを送信するよう制御する制御ステップと、

前記端末装置において、前記最終回のトランザクション処理において  
コミットメッセージの送信する送信ステップと

前記サーバ装置において、連続する複数回のトランザクション処理に  
おける2回目以降の要求メッセージと共に前記コミットメッセージの代  
20 わりに送信される1ビットのフラグであって、端末装置においてラン  
ザクションを処理中であるか処理済みであることを示すトランザクション  
識別フラグを受信するステップと、

前記サーバ装置において、受信されたトランザクション識別フラグに  
基づいて1つのトランザクションの完了を確定するか否かを判定する判  
25 定ステップと

を有することを特徴とするトランザクション処理方法。

29. 要求メッセージの送信、応答メッセージの受信、1つのトランザクション完了を確定させるためのコミットメッセージの送信を含むトランザクション処理に基づいてサーバ装置からコンテンツの利用に対する  
5 ライセンスを取得し、前記ライセンスに基づいて前記コンテンツの利用を制御する端末装置においてトランザクション処理を実行させるプログラムであって、

現在のトランザクション処理について処理中であるか処理済みであるかを示す1ビットのトランザクション識別フラグを保持する保持手段と、  
10 連続する複数回のトランザクション処理における最終回を除く各トランザクション処理においてコミットメッセージを送信しないで、2回目以降の要求メッセージの送信時に、コミットメッセージの代わりに前記トランザクション識別ビットを送信する送信手段と  
を端末装置内のコンピュータに実現させるプログラム。

15

30. 要求メッセージの受信、応答メッセージの送信、1つのトランザクション完了を確定させるためのコミットメッセージの受信を含むトランザクション処理に基づいて端末装置にコンテンツの利用に対するライセンスを提供するサーバ装置においてトランザクション処理を実行させる  
20 プログラムであって、

連続する複数回のトランザクション処理における2回目以降の要求メッセージと共に前記コミットメッセージの代わりに送信される1ビットのフラグであって、端末装置においてトランザクションを処理中であるか処理済みであるかを示すトランザクション識別フラグを受信する受信  
25 手段と、

受信されたトランザクション識別フラグに基づいて1つのトランザク

ションの完了を確定するか否かを判定する判定手段と

をサーバ装置内のコンピュータに実現させるプログラム。



## 要 約 書

本発明のコンテンツ配信システムは、要求メッセージの受信、応答メッセージの送信、トランザクション完了を確定させるためのコミットメッセージの受信を含むトランザクション処理に基づいて端末装置にコンテンツの利用に対するライセンスを提供するサーバ装置と、前記サーバ装置から取得した前記ライセンスに基づいて前記コンテンツの利用を制御する端末装置とを含み、前記端末装置は、現在のトランザクション処理について処理中であるか処理済みであるかを示す１ビットのトランザクション識別フラグを保持する保持手段と、連続する複数回のトランザクション処理における最終回を除く各トランザクション処理においてコミットメッセージを送信しないで、２回目以降の要求メッセージの送信時に、省略されたコミットメッセージの代わりに前記トランザクション識別ビットを送信する送信手段とを備え、前記サーバ装置は、連続する複数回のトランザクション処理における２回目以降の要求メッセージと共に送信される前記トランザクション識別フラグを受信する受信手段と、受信されたトランザクション識別フラグに基づいて１つのトランザクションの完了を確定するか否かを判定する判定手段とを備える。

図1

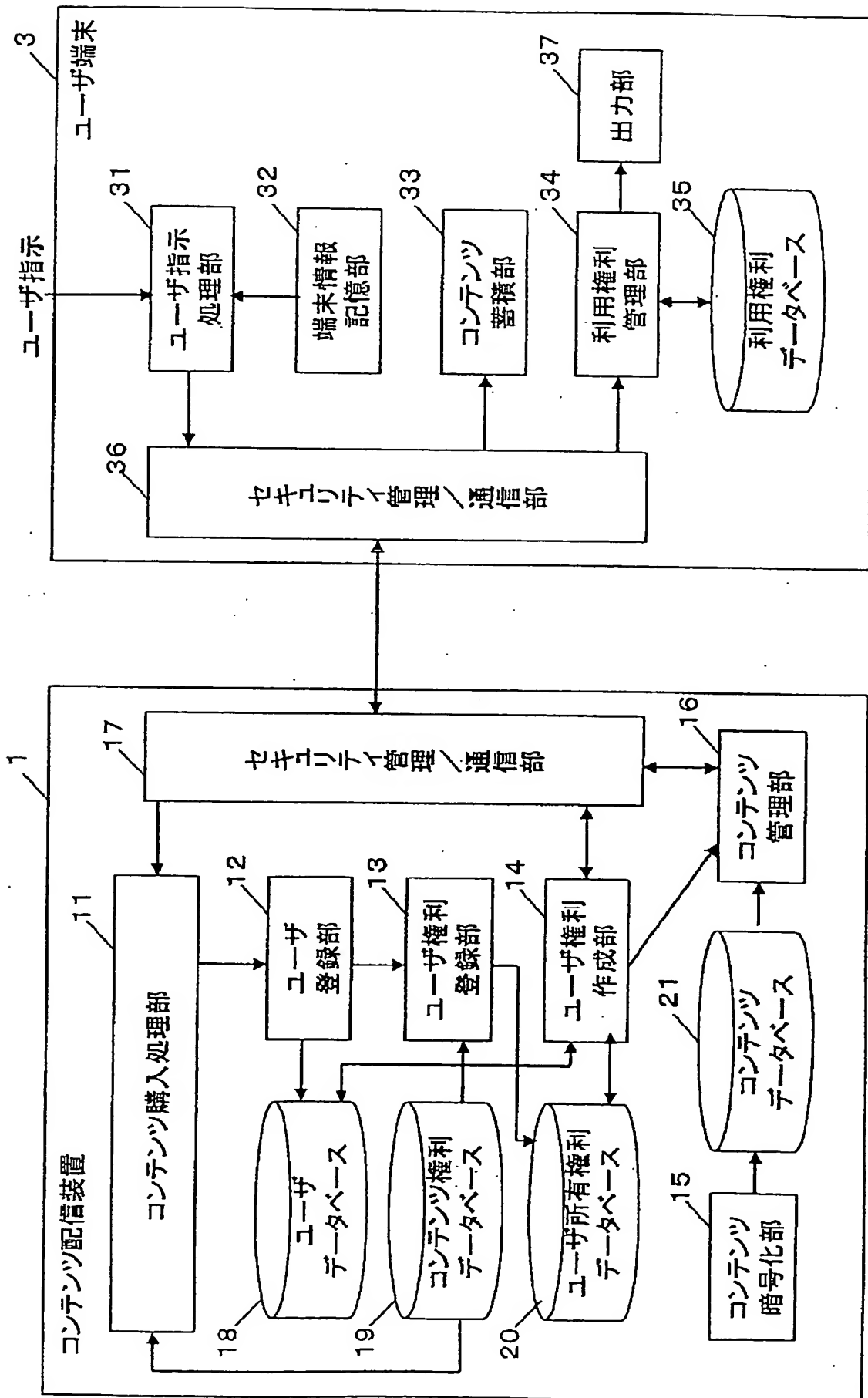


図2

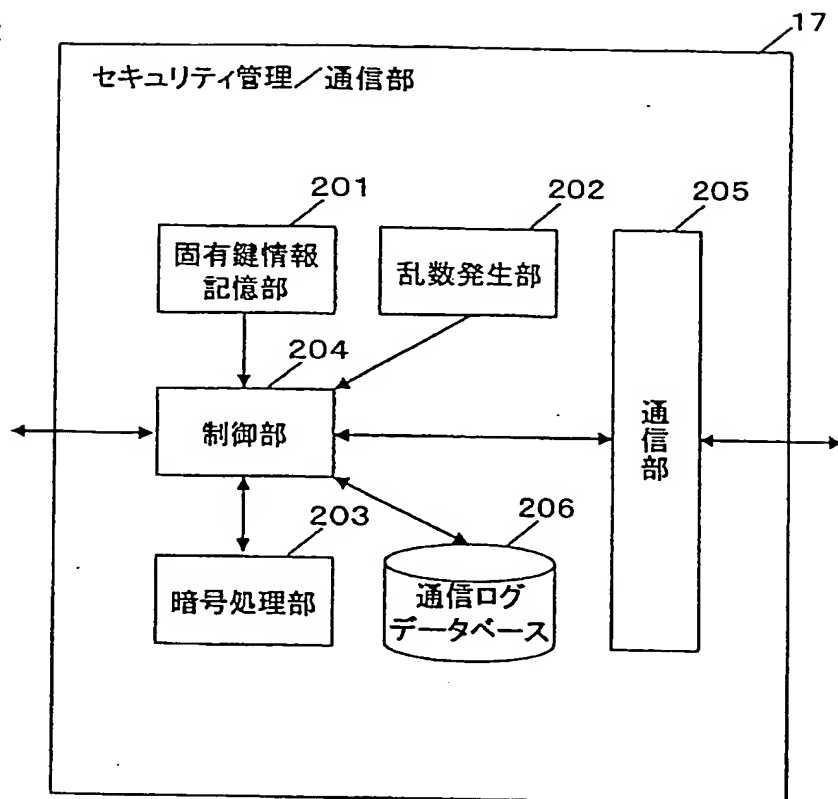


図3

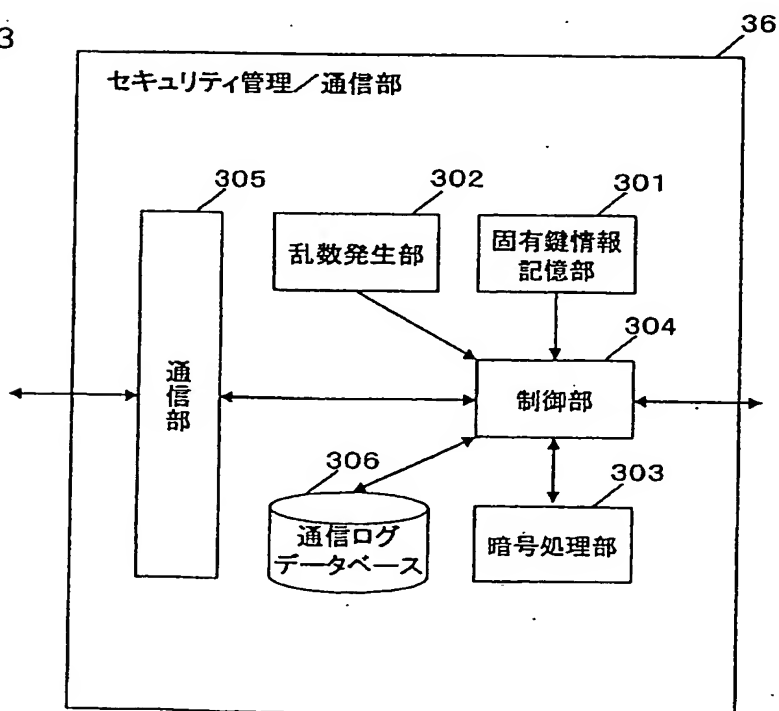


図4

コンテンツ配信装置1

ユーザ端末3

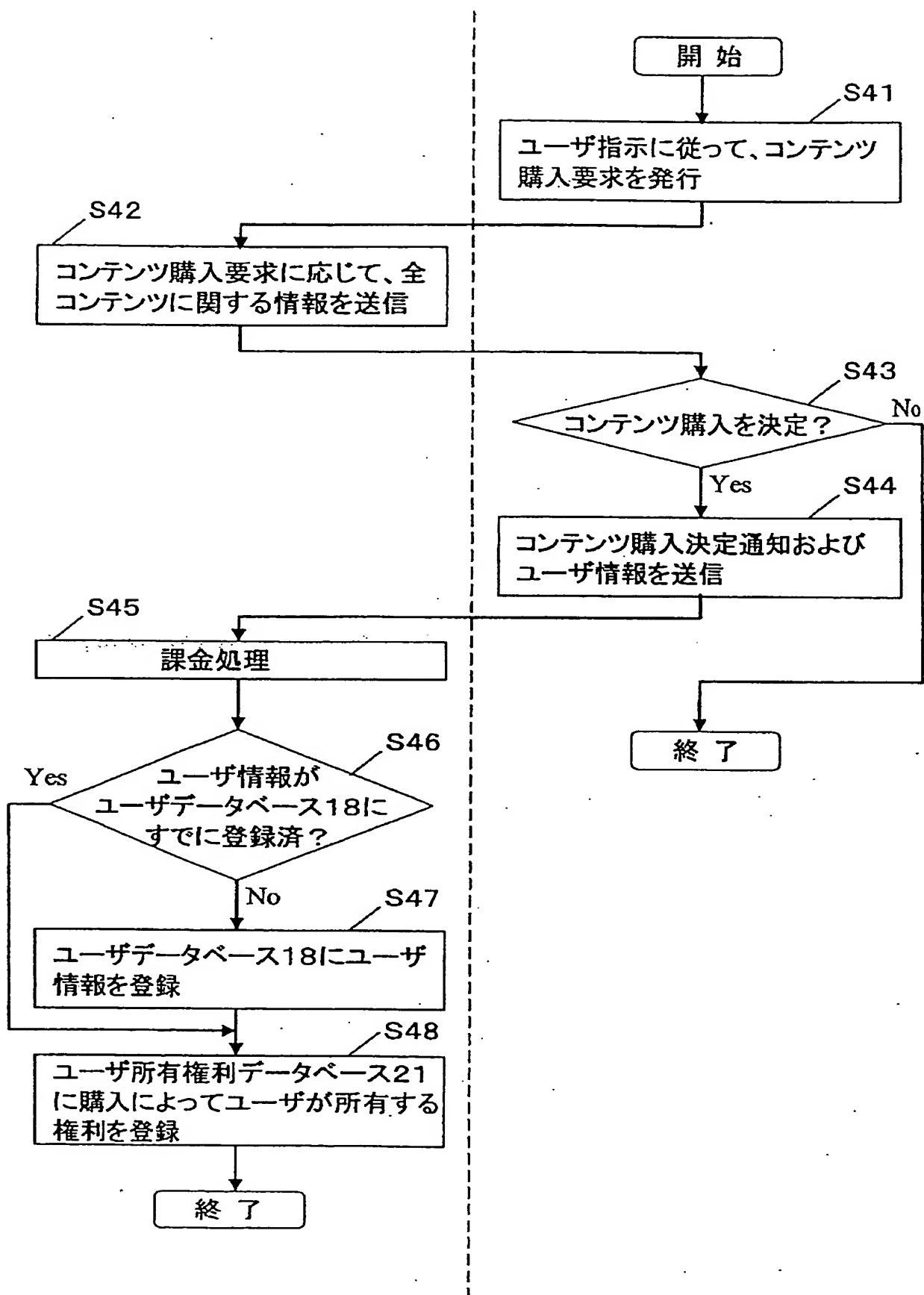


図5

コンテンツ名	コンテンツID	利用条件	料金
映画A	112233	再生回数=2	400円
音楽B	334567	再生回数=5 累積再生時間=1H	500円 1000円
ゲームC	321098	累積再生時間=2H 無制限	700円 2000円

図6

ユーザID	コンテンツID	利用条件
0001	112233	再生回数=2
0002	321098	累積再生時間=2H

図7

ユーザID	コンテンツID	利用条件
0001	112233	再生回数=2
0002	321098	累積再生時間=2H

図8

コンテンツID	コンテンツ名	コンテンツ暗号鍵	ファイル名
112233	映画A	0123456789..	movieA.mpg
234567	音楽B	7361278168..	musicB.wav

図9

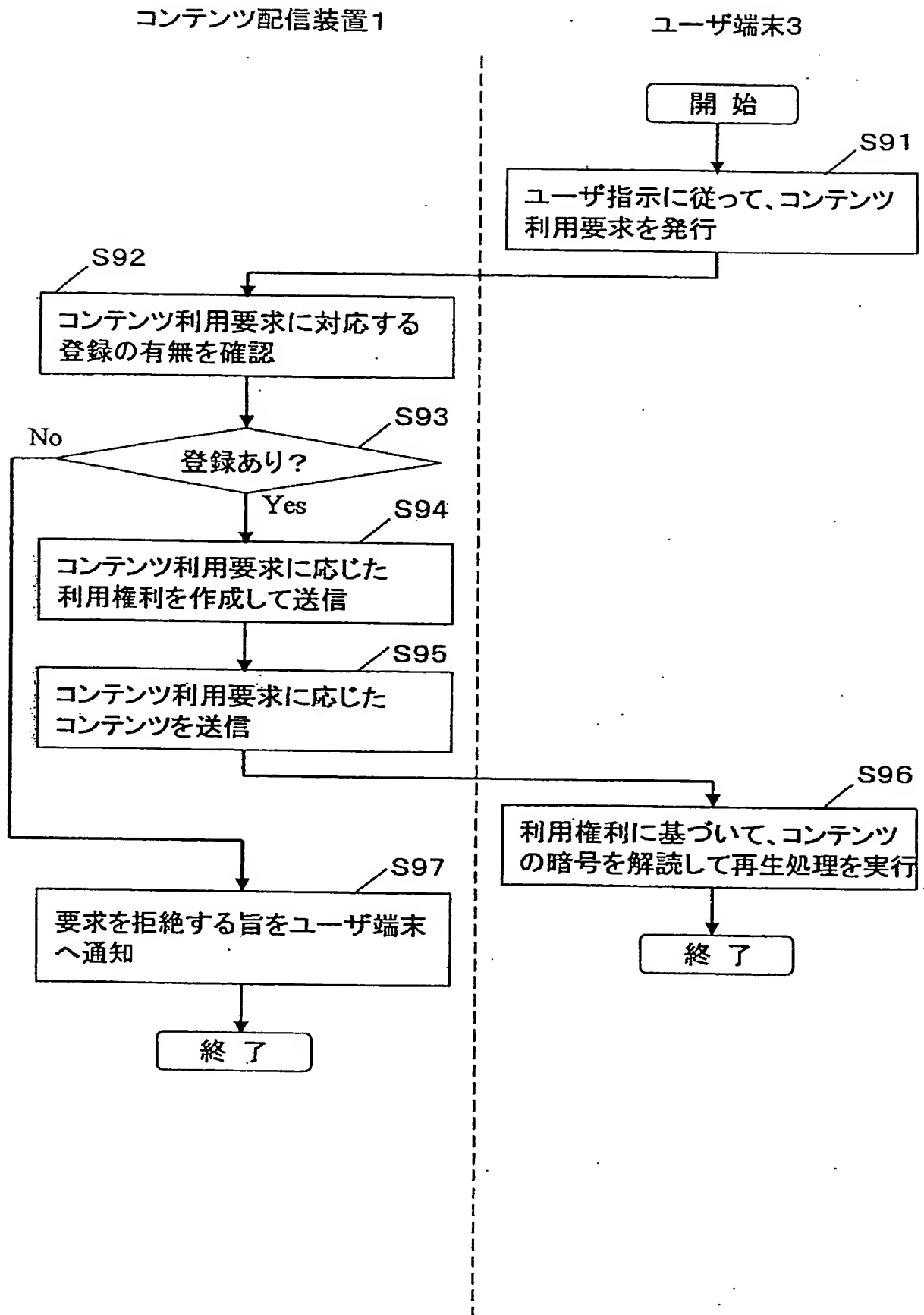


図10A

コンテンツ配信装置1

ユーザ端末3

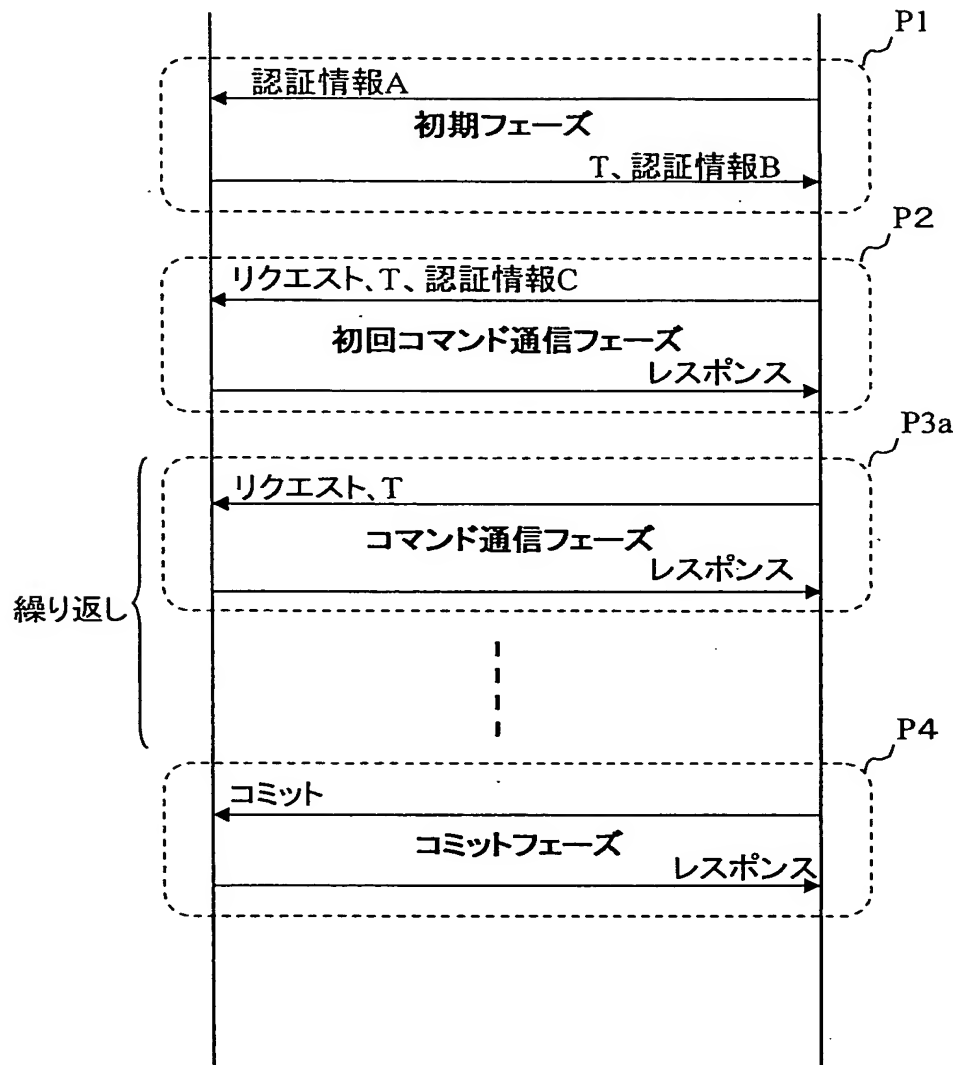


図10B

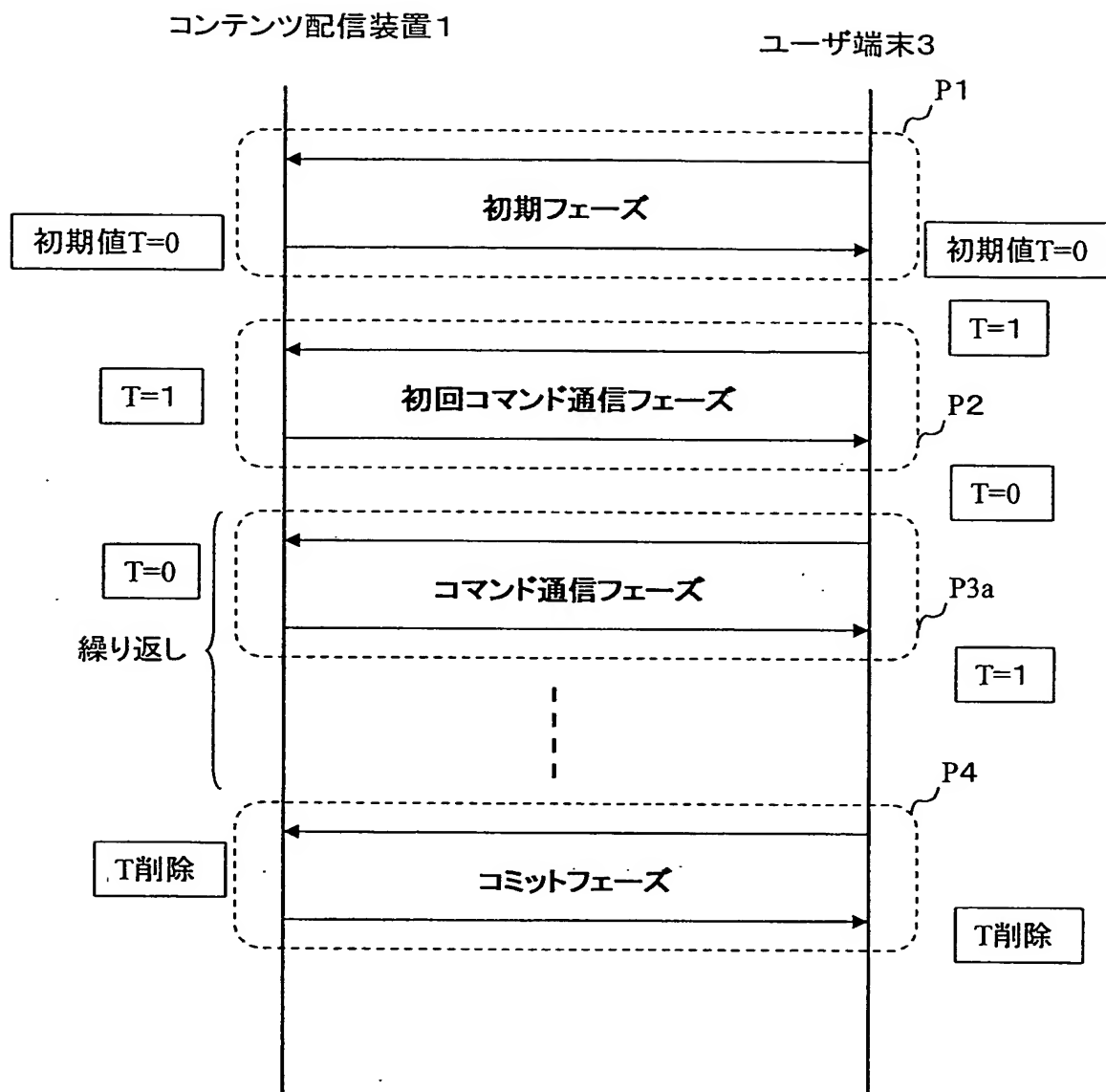




図10C

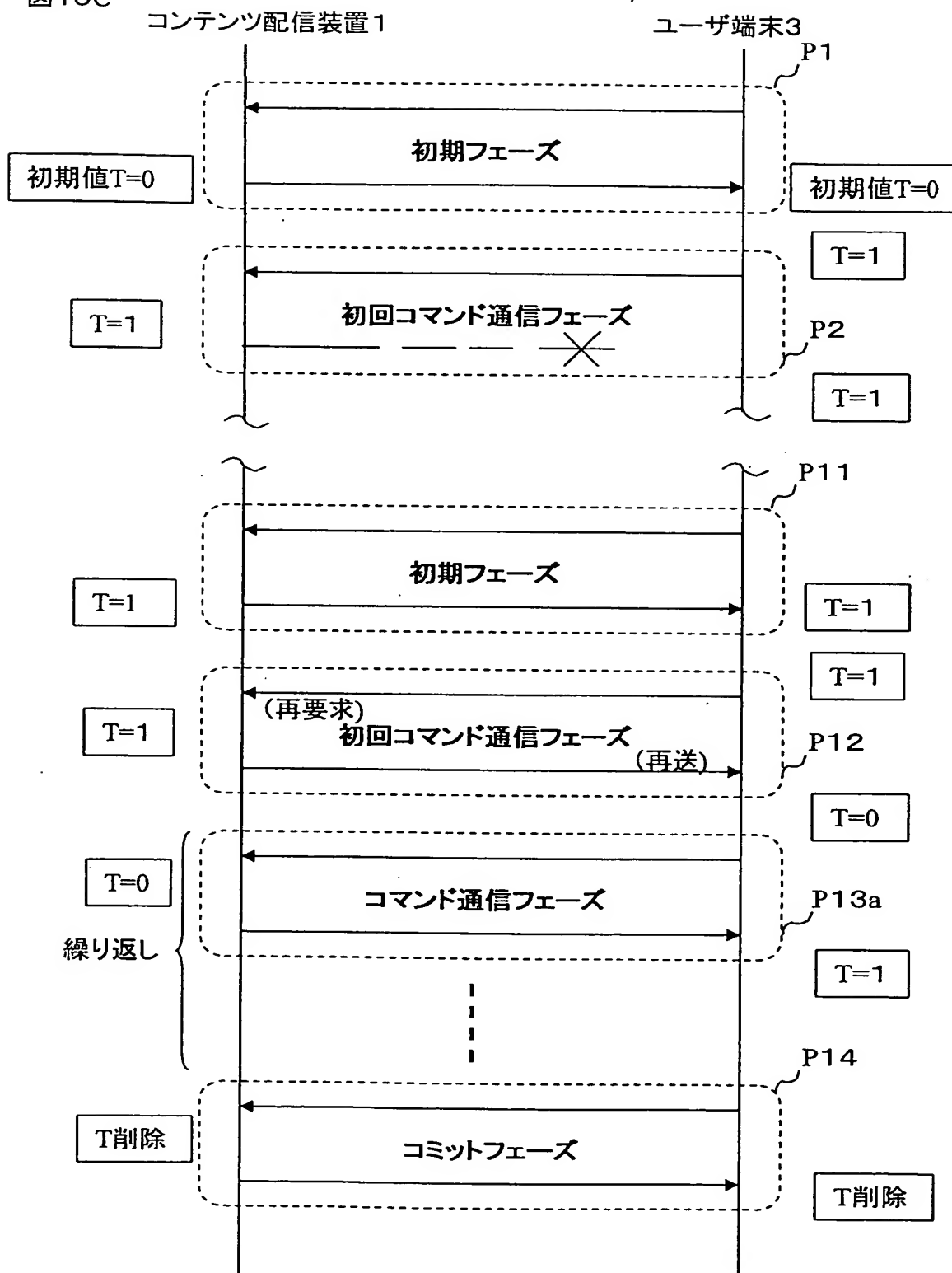


図10D

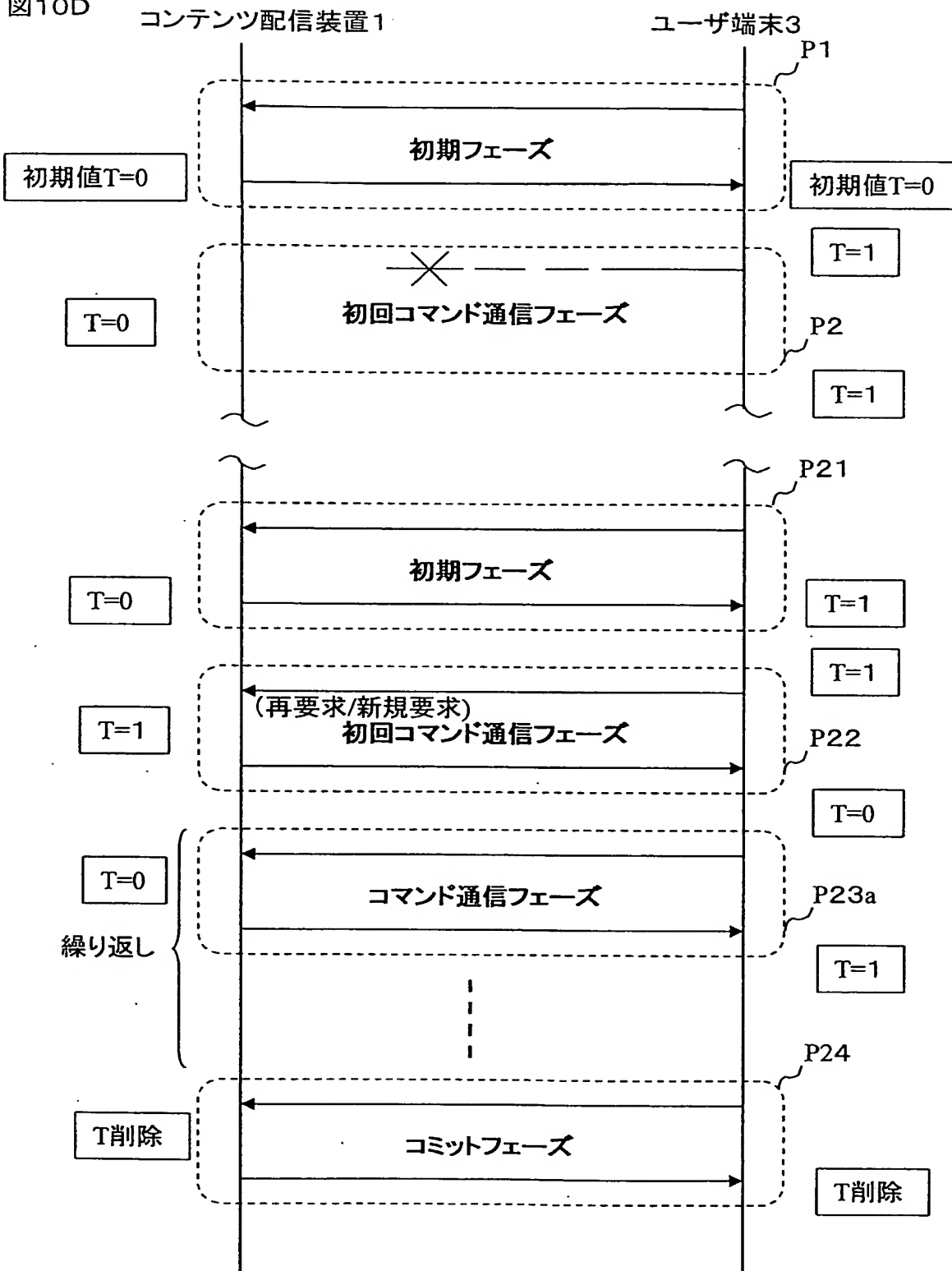


図11

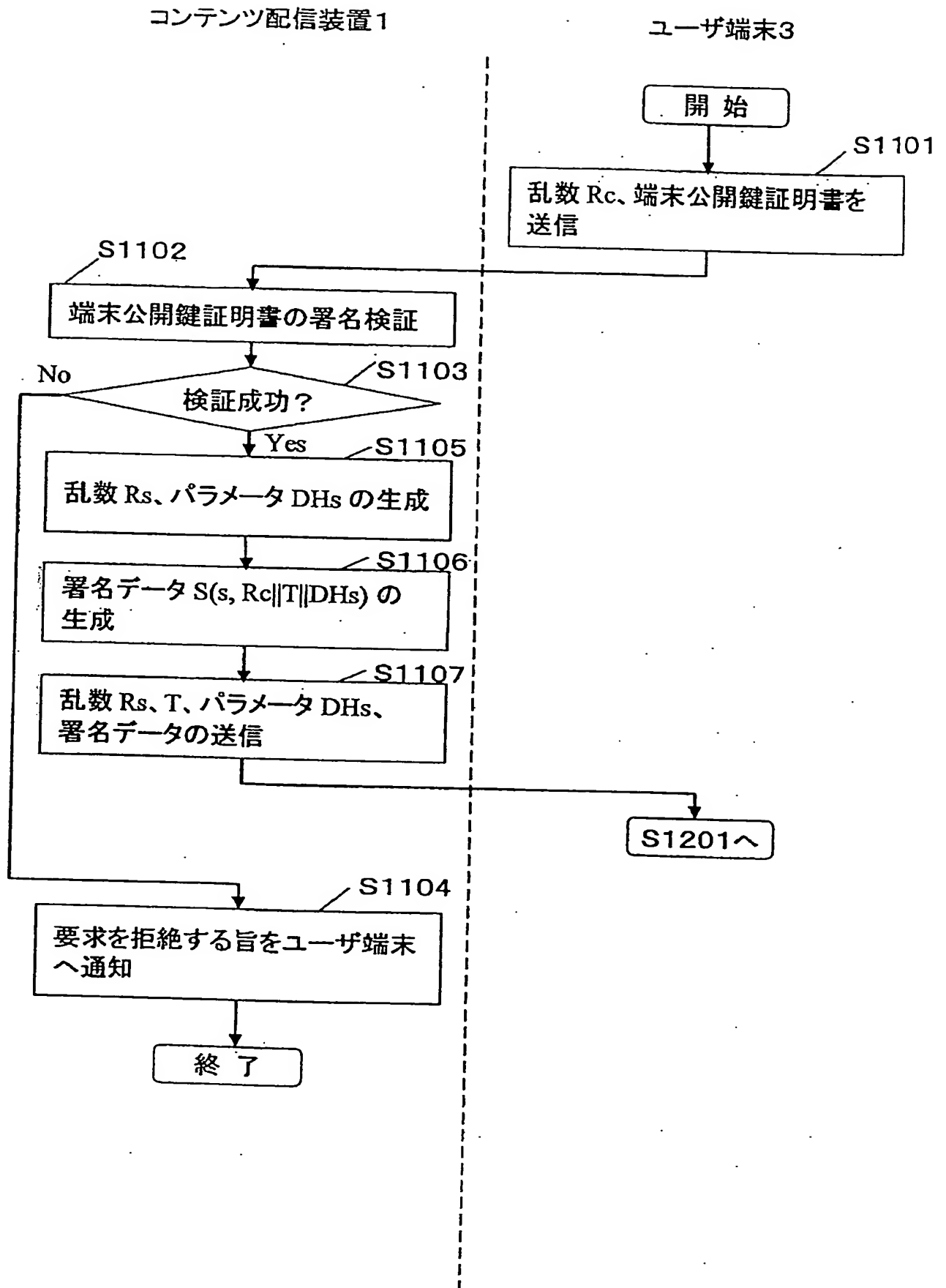


図12

コンテンツ配信装置1

ユーザ端末3

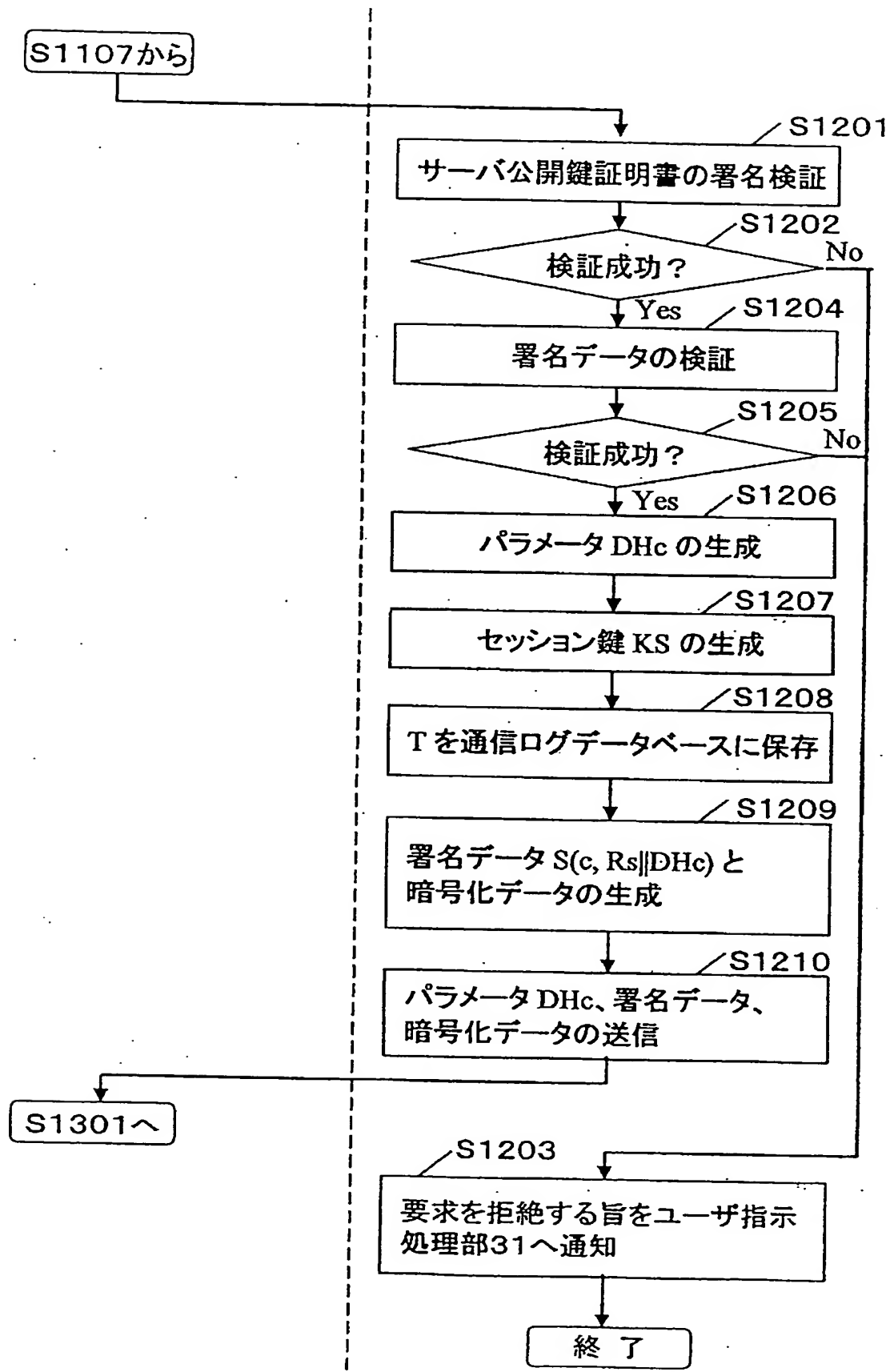


図13

コンテンツ配信装置1

ユーザ端末3

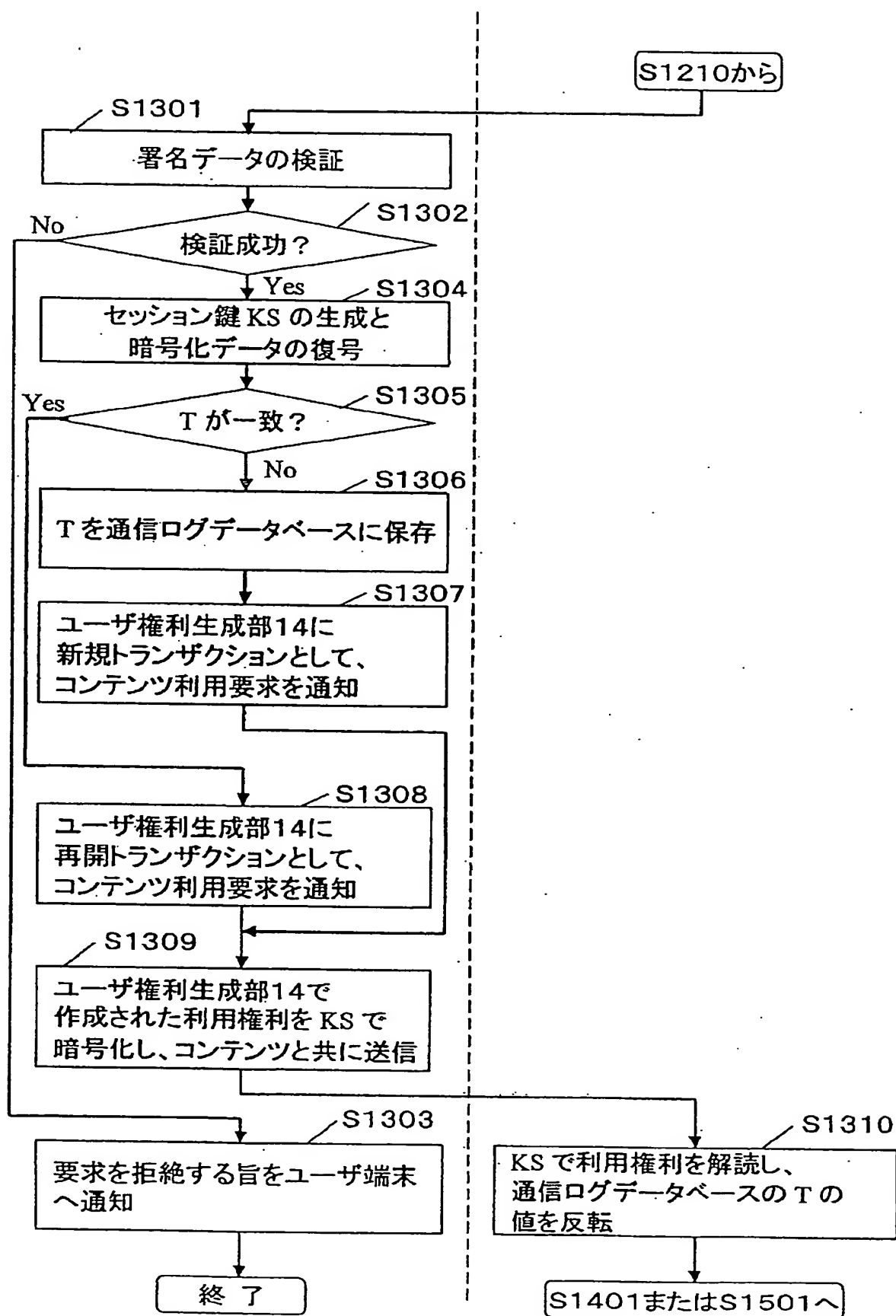


図14

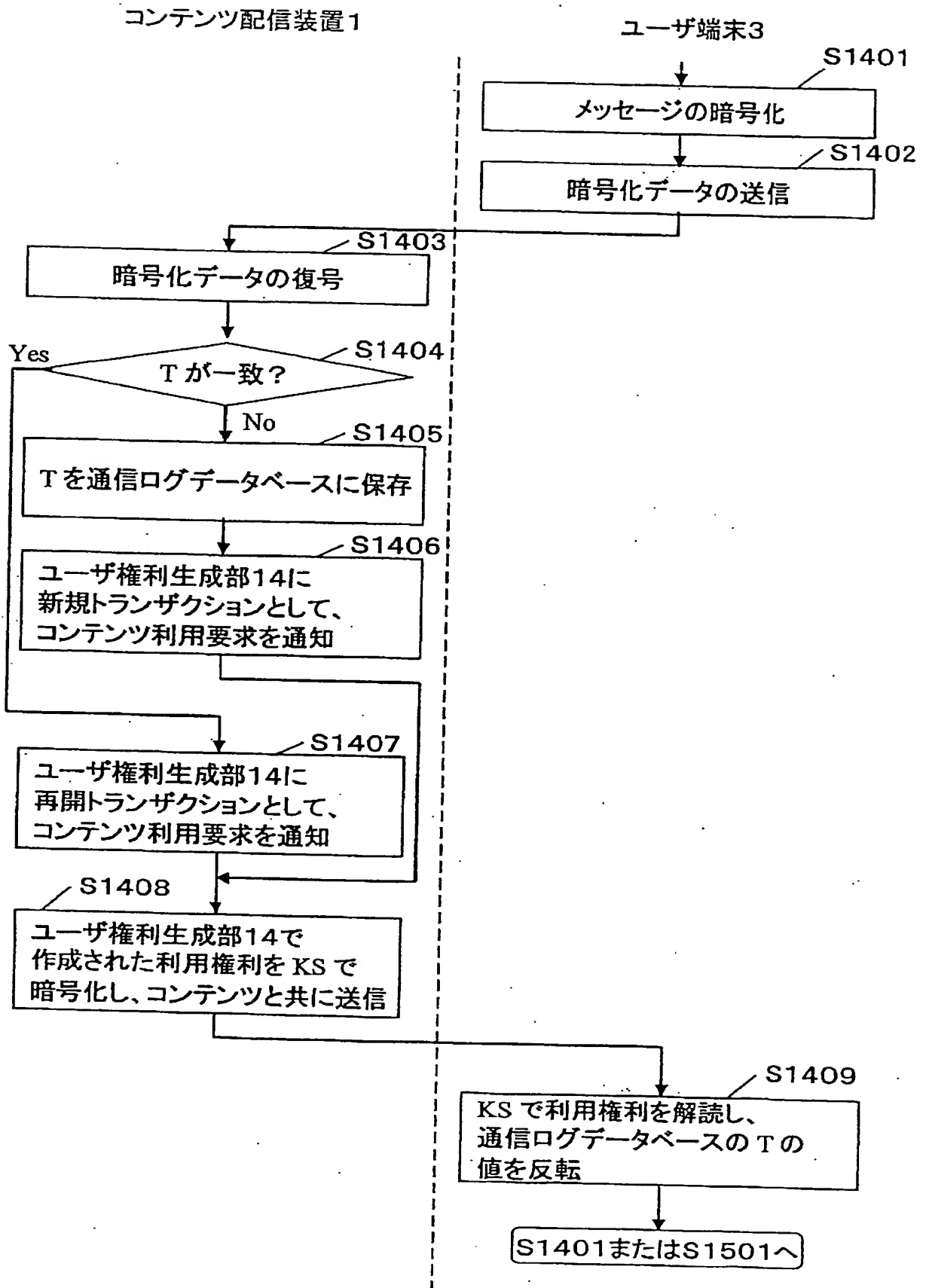


図15

